SHARE@ WORK 2016

MONITORING DIGITAL RIGHTS AND FREEDOMS IN SERBIA

SHARE FOUNDATION

SHARE@ WORK 2016

MONITORING DIGITAL RIGHTS AND FREEDOMS IN SERBIA

SHARE FOUNDATION

IMPRESSUM:

SHARE@WORK 2016: MONITORING DIGITAL RIGHTS AND FREEDOMS IN SERBIA
SHARE FOUNDATION
APRIL 2017
EDITORS IN CHIEF: DJORDJE KRIVIKAPIC, VLADAN JOLER
AUTHORS: DJODJE KRIVOKAPIC, JELENA ADAMOVIC, PETAR KALEZIC, DANILO KRIVOKAPIC, NEVENA KRIVOKAPIC, SONJA MALINOVIC, BOJAN PERKOV, ANDREJ PETROVSKI
OUTPUT EDITOR: MILICA JOVANOVIC
ENGLISH TRANSLATION: MILICA JOVANOVIC
PROOFREADING: ANDREJ PETROVSKI
DESIGN AND LAYOUT: OLIVIA SOLIS VILLAVERDE

PROJECT SUPPORT:

European Commission

Kingdom of the Netherlands

FOND ZA OTVORENO DRUŠTVO - SRBIJA
FUND FOR AN OPEN SOCIETY - SERBIA

Министарство трговине, туризма
и телекомуникација

CIVIL
RIGHTS
DEFENDERS

THIS PROJECT IS FUNDED BY THE EUROPEAN UNION

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of the SHARE Foundation and can under no circumstances be regarded as reflecting the position of the European Union.

1. INTRO-DUCTION

1.1. ABOUT SHARE FOUNDATION

After a series of successful SHARE Conferences on internet culture and activism, with over a thousand participants in Belgrade, Serbia (2011, 2012) and Beirut, Lebanon (2012), participants who cooperated and exchanged experience in these events, interested in running continual research and advocating for human rights in the digital environment, formed a community. As a nonprofit organization, the SHARE Foundation was established in 2012 to advance human rights and freedoms online and promote positive values of an open and decentralized Web, as well as free access to information, knowledge, and technologies. The SHARE Foundation's primary areas of activities are freedom of speech online, data privacy, digital security, and open access to knowledge and information.

Our multidisciplinary team consists of legal and IT experts, artists and journalists. The Foundation has so far organized dozens of conferences, gatherings and workshops in Serbia and abroad, attended by leading activists and experts in digital rights and freedoms. As a contributing member of civil society, the SHARE Foundation participates in public debates on relevant laws that might affect citizens' online rights in Serbia. The Foundation has also produced a dozen of info-guides and other free publications. In the last two years, the Foundation's research branch, the SHARE Lab, published several studies on the internet's invisible infrastructures in Serbia, information warfare, email communication metadata, online election campaigns, Facebook's algorithm factories, and so on. In order to draw more public attention to the importance of human rights online, the SHARE Foundation embarked on producing a 10 episode documentary TV series on some of its core subjects, such as freedom of expression, privacy, new media and digital security, with over 50 local and international experts sharing their insights.

Since March 2017 the SHARE Foundation is a member of European Digital Rights (EDRi), an association of over 30 civil and human rights organizations from across Europe. The Foundation is also a member of the #newmednet, an informal network of lawyers, journalists, activists, and scholars from 14 countries of Central and Southeast Europe, established in 2013, and a member of the Global Net Neutrality Coalition. After three years of providing free legal and technical assistance to online media and civil society organizations, in April 2017 the SHARE Foundation formally registered the first Special Computer Emergency Response Team (CERT) in Serbia.

The SHARE Foundation's activities in promoting online rights were recognized by the Commissioner for Information of Public Importance and Personal Data Protection who in January 2017 presented the Foundation with a letter of gratitude for outstanding contribution to affirming the right to personal data protection.

1.2. ICT USE IN SERBIA

RECOMMENDATIONS

To draft and adopt strategic documents for broadband access development and digital inclusion. To conduct continuous, comprehensive research on the use and implementation of ICT within general and segmented population. To establish a "digital dialogue" of public administration, academia, industry, and the civil sector, in terms of identifying problems and development priorities, as well as models of enforcing domestic law on the internet.

1.2.1. GENERAL POPULATION: DIGITAL GAP AND DELAYED GROWTH

According to the latest data of the Statistical Office of the Republic of Serbia, out of some seven million citizens[1] a little over 64% have internet access, while some 86% of citizens with online access use the internet every or almost every day.[2] The behavior, habits and trends of internet use, however, are rarely a subject of research. There are some periodical statistics of global internet traffic, or occasional polls by local private actors, of unknown methodologies. But scientific research focused on particular strata of the community, beyond mere opinion polls, is among the rarest source of data.

The official statistics undoubtedly reveal a deepening digital gap – a socioeconomic risk endangering free and balanced access to digital technologies. These disparities within the society are most obvious among marginalized and vulnerable groups, such as persons with disabilities, ethnic Roma population, and citizens in rural areas. At the same time, slow growth and delayed ICT development keep Serbia on the struggling side of the global digital divide.

The new World Bank regional report for Europe and Central Asia, published in March 2017, puts Serbia among European countries with the

[01] Estimated population in January 2016: 7,076,372 http://www.stat.gov.rs/WebSite/Public/PageView.aspx?pKey=2

[02] Usage of Information and Communication Technologies in the Republic of Serbia, 2016 http://pod2.stat.gov.rs/ObjavljenePublikacije/G2016/pdfE/G20166004.pdf

highest prices for fixed internet (more than US$25 per Mbit per month, in purchasing power parity [PPP]).[3]

In 2009 the Serbian government adopted a national strategy of broadband internet access development, along with an action plan to meet its objectives by 2012. These documents provided measures for improving social inclusion: forming a telecom ducts cadastre and drawing up a plan for efficient use of telecommunications infrastructure; creating models for faster development of the broadband access market; unifying the network of elementary and secondary schools and integrating cultural institutions in the academic network; enabling public broadband access at government and public premises, etc. The measures were not implemented. The ministry in charge drafted a new broadband internet strategy by the end of 2013, but it was never brought to a conclusion. At a panel discussion held at the Belgrade Chamber of Commerce in early 2017, it was said that the state has no funds available but that incentives are to be made for service providers to invest their own resources in broadband development, with an immediate goal of 70% of territory coverage.[4]

The national Statistical Office survey on ICT usage shows that 65.8% of households in Serbia own a computer, which is an increase of 1.4% and 2.6% compared to 2015 and 2014, respectively.[5] The percentage of households owning a computer varies across the territory: in Belgrade it amounts to 75.9%, in Vojvodina 67.7%, and in Central Serbia 59.4%. The differences are also visible when comparing the availability of computers in urban and rural areas of Serbia: 73.3% versus 54%. Statistics show that this gap has significantly increased since 2015, comparing the growth rates of computer availability in urban (2.2%) and rural (0.1%) parts of Serbia.

The most drastic digital gap is recorded within the population with disabilities that, according to the 2011 census makes 8% of the overall population in Serbia. As stated by the Report on Digital Inclusion, 90.2% of the population with disabilities use neither a computer nor the internet. There are only 5% computer literate persons in the total population with disabilities, while less than 9% use the internet.[6]

Speaking of the general population in Serbia, the national Statistical Office survey shows that 64.7% of households have internet connection, which is an increase of 0.9% and 1.9% compared to 2015 and 2014, respectively. The highest percentage of internet connection households was observed in Belgrade (73.1%), followed by the region of Vojvodina (68.7%), while Central Serbia has the lowest percentage (57.9%).

For comparison, the majority (55%) of households in the EU-28 had internet access in 2007, while the share of EU-28 households with internet access reached 85% in 2016. The highest proportion (97%) of households with internet access in 2016 was recorded in Luxembourg and in the Netherlands, and the lowest rate of internet access among the EU Member States was observed in Bulgaria (64%).

Income discrepancy is a significant factor in accessing internet in Serbia. The internet connection is mostly used by households with over 600 EUR of monthly income (94.7%), whereas only 46.1% of households with under 300 EUR income are connected to the internet.

In regard to the devices used, households in Serbia most often use mobile phones (76.5%), 72% use personal computers, and 49.3% use laptops. The number of households that access the internet via mobile phone increased by 8.6% compared to 2015. Of the total number of households with internet connection, 45.5% have DSL (ADSL), 45.3% use cable internet, and 1.2% have a modem or ISDN connection.

Some 57% of households in Serbia have a broadband internet connection which, according to statistics, is an increase of 1.8% and 2.7 % compared to 2015 and 2014, respectively. This type of internet connection is mostly used in Belgrade (68.5%), in Vojvodina (61.0%), and the least in Central Serbia (50.4%). In comparison, 83% of the households in the EU had a fixed and/or mobile broadband connection in 2016.

Results of the national Statistical Office survey on ICT usage in enterprises indicate that 99.8 % of enterprises operating on the territory of the Republic of Serbia use computers for their business. 98.6% of enterprises use public e-services, which is an increase of 4.1% and 6.6% compared to 2015 and 2014, respectively. There are 1.4% of enterprises that do not use this possibility. In 2015, 41% of enterprises ordered goods/services online, which is a decrease of 0.7% compared to 2014 and an increase of 0.6% compared to 2013. Official statistic shows that in 2015 only 23.3% of enterprises received orders online (excluding e-mails). 9.3% of enterprises pay cloud computing services. [9]

[03] "Reaping Digital Dividends: Leveraging the Internet for Development in Europe and Central Asia", p 63. https://openknowledge.worldbank.org/bitstream/handle/10986/26151/9781464810251.pdf

[04] "Computer usage in Serbia", TV N1, January 2017 [in Serbian] http://rs.n1info.com/a224076/Sci-Tech/Upotreba-racunara-u-Srbiji.html

[05] Usage of Information and Communication Technologies in the Republic of Serbia, 2016 http://pod2.stat.gov.rs/ObjavljenePublikacije/G2016/pdfE/G20166004.pdf

[06] Report on Digital Inclusion in the Republic of Serbia 2011-2014 [in Serbian] http://socijalnoukljucivanje.gov.rs/wp-content/uploads/2015/03/Izvestaj-o-digitalnoj-ukljucenosti.pdf

[07] Digital economy and society statistics – households and individuals http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital _ economy _ and _ society _ statistics _ - _ households _ and _ individuals

[08] Internet access and use statistics - households and individuals http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet _ access _ and _ use _ statistics _ - _ households _ and _ individuals

[09] or comparative EU data: Digital economy and society statistics – enterprises http://ec.europa.eu/eurostat/statistics-explained/index.php/Digital _ economy _ and _ society _ statistics _ - _ enterprises

1.2.2. TRAFFIC AND TRENDS

Citizens of Serbia obviously spend much of their time online visiting several larger news portals and social media, but it is yet unclear what they are doing there – do they prefer reading texts or watching news videos; are they more interested in readers' comments, message boards or other, commercial sections of online media? It is also unknown how many unique visits are in fact generated through infected devices, turned into bots. [10]

Statistics say that a little over three million citizens of Serbia use internet every day, or almost every day.[11] According to Alexa.com metrics, which include global services and their localized versions, three most popular internet services in Serbia are Google Search, Youtube, and Facebook. News portal Blic.rs is the first native language site on this list (fifth place[12]), followed by Wikipedia and the adult webcam platform Bongacams[13]. Within 20 most visited sites there are two search engines, two social media, five online media, five collaboration platforms, and four e-trading platforms.

There is also a monthly chart of the most visited websites in Serbia issued by the local branch of the Gemius company with disputable metrics results,[14] but similar to the Alexa's global index. Taking only desktop traffic into account, the top three native language websites according to the January 2017 chart, were those of the national media – Blic.rs (1,837,924 real users), Kurir.rs (1,511,200) and B92.net (1,089,862).[15] Based on the Gemius' chart, the fourth place was occupied by a classifieds website, kupujemprodajem.com with 1,001,838 real users. Next in this category was a website advertising used cars, polovniautomobili.com (seventh place, 679,079 real users). Among the top ten in January 2017 there were two more media websites, a tabloid Telegraf.rs and Vecernje Novosti daily.

Due to the lack of data for previous years[16] it is not possible to track visits in the context of various vectors of influence, such as growth rates in internet usage, new legal provisions regulating various online activities, or mass occurrences of astroturfing, aimed at larger news portals.

[10] Devices infected with malicious software perform repetitive operations such as automated 'liking', posting, rating comments, and alike.

[11] Usage of Information and Communication Technologies in the Republic of Serbia, 2016 http://pod2.stat.gov.rs/ObjavljenePublikacije/G2016/pdfE/G20166004.pdf

[12] Google appears twice under different top domains: .rs and .com.

[13] Top sites in Serbia http://www.alexa.com/topsites/countries/RS

[14] In March 2017 the national association of digital advertisers (Interactive Advertising Bureau, IAB Serbia) publicly warned Gemius.rs of irregularities in measuring local internet traffic, demanding corrections as of December 2014. Reliant data for mobile and total traffic are expected in May 2017, while desktop traffic data could be deemed reliable [in Serbian] http://iab.rs/en/saopstenje-iab-serbia-komiteta-za-audience-measurement/

[15] Gemius Audience http://www.audience.rs/; visits are not geographically layered

[16] In the first half of 2015 Gemius' local chart appears to be a random list, with no measurable indicators.

According to unofficial statistics that count on some 4,7 million internet users in Serbia, almost 3.5 million use Facebook: it is the choice of 91.52% of social media users, whereas Twitter, despite having a particular status in the public sphere for enabling instant and searchable exchanges, draws only 4.06% of social media users in Serbia.[18]

Although various digital tools made tracking subjects and keywords circulating in public much easier, there is still little data that would shed more light on themes discussed by online communities in Serbia. Some indication of public discourse content could be drawn from the annual statistics of global services or their tools, such as Google Search: "We mostly search for fun and ways to spend our free time (online games and entertainment sites dominate with total of 20 search keywords). Communication and online work tools come in second (17 keywords), and the third are media and information with a total of 15 keywords." [19]

1.2.3. INTERNET AND TERRITORIAL JURISDICTION IN SERBIA

The regulatory reach Serbia has on the internet can be determined by examining 100 websites that Serbia's citizens visit mostly, based on global index Alexa.

An immediate observation tells that less than one quarter of the websites most visited in Serbia (24 of them) have registered a national top domain .rs, while the rest have top-level domains such as .com (59) .net (8) .org (2), etc.

As for registered domain owners, 15 out of top 100 have made their contact information private, while out of the known domain owners, 35 are located on the Serbian territory, 29 are based in the US, five other jurisdictions have two known owners each (Ireland, Croatia, Malta, Kosovo, UK), and the rest is scattered across 11 other countries.

As for persons in charge of administration, 10 websites have no information regarding that, 40 provide the same name under administrative contact as the registrant, while 50 show some differences, whether due to a 'parent-subsidiary' company relations or if no clear relation can be established, between the domain registrant and the person in charge of administration. By reviewing known administrators, it could be said that about one third comes from the US (34) and Serbia (33), while the rest are located in the UK (4), Malta, Canada, Kosovo, Cyprus (2), and other countries.

[17] Concealed promotion of political, religious, marketing, or other content, by creating an impression of authentic grassroots opinion and support; in online environment it usually includes organized commenting, sharing, voting, and alike.

[18] Social Media Stats in Serbia http://gs.statcounter.com/social-media-stats/all/serbia/#monthly-201702-201702-bar

[19] "What did Serbia googled in 2016" [in Serbian] http://genuine.rs/sta-je-srbija-guglala-u-2016

By looking at the hosting services which the top 100 websites use, almost half of them chose US companies (48), less than one quarter placed their trust with Serbian hosting companies (23), followed by hosting services in Germany and the Netherlands (7 each).

Finally, using diagnostic tools for tracking transit (traceroute), one can establish the location of the servers that make the content of these websites available online. The results show that two-fifths out of top 100 websites are based on servers physically located in the US (40), over one quarter are in Serbia (27), while the Netherlands (9) and Germany (8) prove to be popular in this category also for internet companies operating outside their home country.

While 60% of the most visited websites have no established connection to Serbia, those websites that hold at least one criteria connection usually meet other criteria too. Thus, it could be said that for 40% of the top 100 websites Serbia has some sort of jurisdiction over domain registrants, website administrators, hosting companies and/or servers. In those cases, local officials could claim authority to regulate those websites' content.

In a more detailed analysis of 60 websites with no established connection to Serbia by the described criteria, two thirds (41 out of 60) show no relation to Serbia at all, while one third (19) have some sort of local business presence (the website is available in the Serbian language, there is a registered national domain besides the main domain, there are partners in Serbian territory, etc.). Concerning those 19 websites, the Republic of Serbia could establish its jurisdiction provided that the international instruments of cooperation are used to secure enforcing a decision. As for the 41 websites with no relation to Serbia whatsoever, every attempt to regulate and enforce a certain policy would depend on cooperation of international partners.

Therefore, 40% of the 100 most visited websites clearly fall under Serbian jurisdiction, and it is reasonable to expect that they comply with national regulation; 20% have their businesses present locally, and again it is reasonable to expect their compliance with Serbian laws at least in related matters. The rest are entirely under the jurisdictions of other countries. In short, the regulatory reach of the Republic of Serbia to the global information system is limited, as well as its influence over the Web on its own territory.

In the context of the limited sovereignty it is important to deal with challenges and models of enforcing the law on the internet, searching for solutions to directly apply the national law online. It is also important to consider prospects of creating a supranational forum acknowledging the significance of unified rules of the international law, and to join efforts in creating a basis for resolving conflicts of law and jurisdiction on the internet.

U kontekstu ograničenog suvereniteta značajno je pozabaviti se izazovima i modelima primene prava na internetu, kao i mogućnostima direktne primene nacionalnog prava na Mreži, potencijalima za kreiranje nadnacionalnog foruma, značajem unifikovanih pravila međunarodnog prava i osnovama rešavanja sukoba zakona i nadležnosti na internetu.

1.3. MONITORING: A GENERAL OVERVIEW

RECOMMENDATIONS

Immediate implementation of measures agreed upon in cooperation of the Ministry of Interior Affairs, the Public Prosecutor's Office, press and media associations. Increasing capacities of the authorities investigating and prosecuting high-tech crime to improve legal certainty concerning those who participate in informing the public. Empowering press associations, self-regulatory bodies, and the media through risk awareness, incident recognition, and raising cybersecurity culture in general.

The SHARE Foundation monitors digital rights and freedoms in Serbia since mid-2014, documenting violations against citizens, journalists, media, and other social actors. The immediate motive to establish continuous monitoring came from a series of incidents that occurred in May 2014, during and after the disastrous floods that hit the region, with cyber attacks removing content and blocking websites, and citizens being taken in for questioning.[20] More than 300 cases have been registered in three years. [21]

In the course of gathering data, SHARE's monitoring team created methodology to process and classify cases of abuse of digital rights and freedoms in Serbia. The violations are processed in regard to specific information of an incident:

1. Target or actor
2. Attacker (if available)
3. Means (e.g. malware) or legal consequence (e.g. criminal charges)
4. Category (e.g. technical attack)
5. Timeline

[20] "Internet remembers all"; SHARE Foundation, 2014 [in Serbian] http://www.share-conference.net/sh/defense/internet-sve-pamti

[21] Monitoring database [in Serbian] http://monitoring.labs.rs/

6. Additional notes (pictures, links, description)

Categories of violation include all types of possible offenses or assaults, even if a specific kind has not yet been registered in Serbia, such as internet or content filtering.

CATEGORIES OF VIOLATION:

A. TECHNICAL ATTACKS AGAINST CONTENT INTEGRITY

1. Unlawful rendering content inaccessible
2. Damaging computer data and programs, data theft, altering content (unlawful deleting, altering, deteriorating, or rendering computer data and programs inaccessible, data sabotage – inputting, damaging, deleting, deteriorating, suppressing or otherwise rendering computer data or programs inaccessible, with the intent to prevent or disturb access to content or system)
3. Computer fraud – inputting false data or not inputting correct data with the intent to alter the result of computer data processing or transmission.

B. ELECTRONIC COMMUNICATION SURVEILLANCE, VIOLATION OF RIGHTS TO PRIVACY AND PERSONAL DATA PROTECTION

1. Electronic surveillance
2. Violation of communication privacy by private actors
3. Violation of personal data protection regulation

C. ABUSING THE RIGHT TO FREE SPEECH, PRESSURE AGAINST ACTIVITIES AND EXPRESSION ONLINE (JOURNALISTS, ONLINE MEDIA, BLOGGERS, ACTIVISTS, INDIVIDUALS)

1. Defamation
2. Insults and value judgments
3. Endangering privacy
4. -Pressure, threats and endangering safety
5. Freedom of expression online and employment

D. ONLINE MANIPULATION

1. False impersonation and identity theft
2. Abuse of digital tools and processes (astroturfing, botnets, etc.)

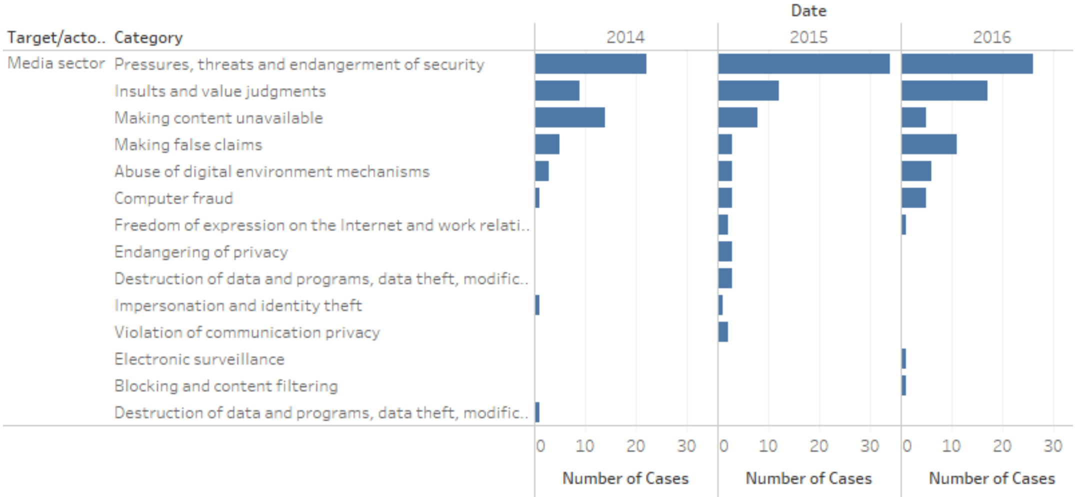
E. MISUSE OF INTERMEDIARY LIABILITY

F. BLOCKING AND FILTERING CONTENT

G. OTHER

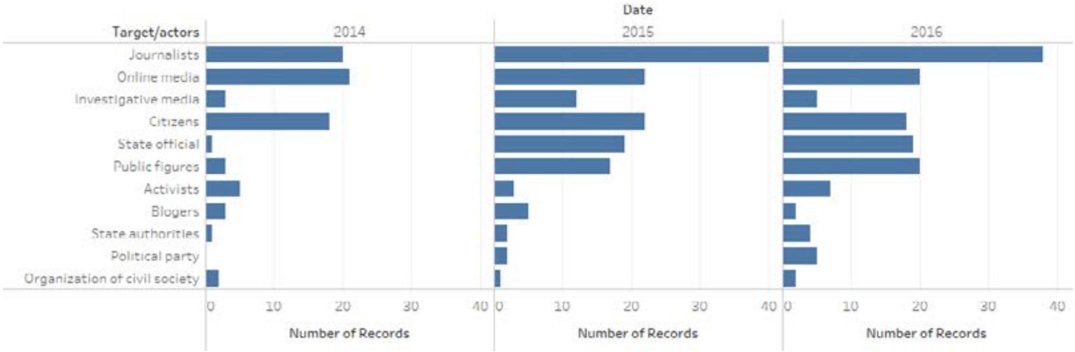
TRENDS

Over the past three years the media and journalists, particularly those engaged in investigative work, have faced mostly threats, pressure, and security risks. There is a downward trend of technical attacks aimed at making online content unavailable.



Number of cases per type of attack (media sector)

Journalists, online media and citizens are the most common targets of digital rights and freedoms violation, with more frequent attacks against investigative media, activists, public figures and state officials.



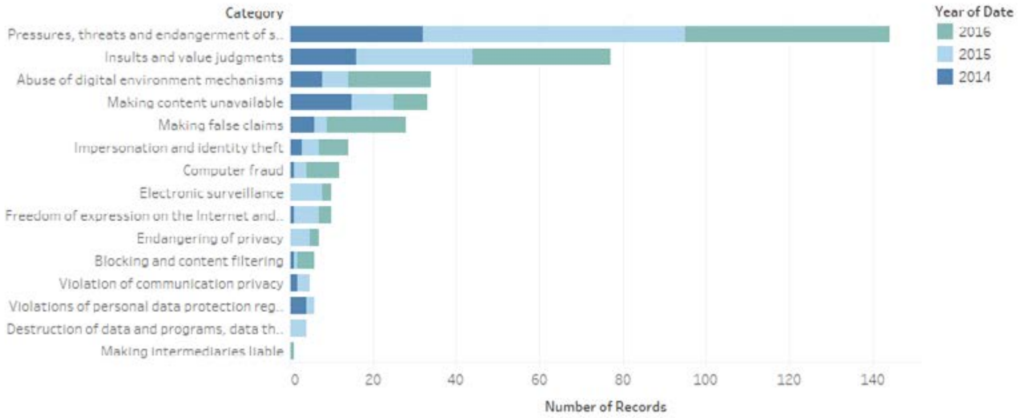
Frequency of attacks per year

1.3.1. RESPECTING RIGHTS AND FREEDOMS ONLINE IN 2016

Incidents in the monitoring database are classified by the type of violation, ranging from technical attacks and privacy breaches to insults and endangering safety. Almost one third of total incidents recorded since the monitoring began were related to pressure and threats to safety. In 2016 the number of these incidents somewhat declined, but it is still relatively high compared to other types.[22]

The beginning of the year was marked by the parliamentary elections held in April. For the first time in Serbia, social media and various sharing platforms played a significant role in promoting political ideas during the campaign. Several political groups (Dveri, Dosta je Bilo, SRS) in fact won seats thanks to online media.[23] Resorting to illicit tactics spread from offline campaigns to the internet, with various tools making manipulative practices easier, such as false impersonation, mudslinging, and alike. Content similar to genuine political messages was distributed, creating confusion and misattribution of views to the racing parties. Particularly detailed was the production of video clips falsely attributed to the radical right movement "Dveri", distributed from a newly setup YouTube channel, aimed at discrediting the movement and manipulating public opinion.

As opposed to the first two years of monitoring, in 2016 there was no increase in the number of cases of compromising online content through technical means - DDoS attacks being most common in local context. Technical attacks carried out in 2014 and 2015 against websites publishing dissenting views (Pescanik, CINS, Teleprompter) were incidents that drew most public attention. None of those cases were resolved in court.



Number of reported cases per category

[22] Digital rights and freedoms in Serbia – 2016 overview; SHARE Foundation, 2016 [in Serbian] http://www.shareconference.net/sites/default/files/u742/godisnji _ monitoring _ izvestaj _ 2016 _ za _ sajt.pdf

[23] "#izbori2016 [#elections2016] Online campaign pays off", SHARE Foundation, 2016 [in Serbian] http://www.shareconference.net/sh/defense/izbori2016-kampanja-na-mrezama-se-isplati

In 2016, the SHARE monitoring team registered about 15 technical cases of violation of rights in the online environment. At least two of those cases involved media ("Danas" daily and "Pistaljka" website) being targeted right after publishing reports related to top state officials and their immediate staff.

On the other hand, there was an increase of cases of social media accounts being locked or suspended, but due to the lack of details most of those incidents cannot be qualified clearly. Such cases were most often reported by users that felt their access has been denied because of their critical views or their social role, most of them being journalists, members of local councils, civil sector and online activists. It remains unclear whether a social media service automatically locks down user accounts for "suspicious activity" or detected attempt of unauthorized access, or due to a number of reports sent by political opponents, under various pretexts of alleged policy violation (hate speech, copyright infringement, etc.).

Experience of the community tells that, at least when Twitter is concerned, a suspended account is relatively easy to unlock if there was no real violation of policies – provided that users remember the email of their initial registration or their old password.

However, non-transparent procedures of suspension or deletion of posts and accounts on social media, Facebook and YouTube in particular, are gaining more attention globally. Big corporations have assumed policing the boundaries of free speech online, with human and algorithmic censors authorized to regulate public space and select information exchange.

Nevertheless, the boundaries between freedom of expression and hate speech, verbal assaults, and threats, remain one of the key topics both globally and locally. Numerous incidents of violation of rights, registered by the SHARE monitoring team in 2016, include abuses of the right to free speech and exerting pressure against online activities by false claims, insults, discredits, degradation, threats to safety, and alike. Compared to 2015, when there were 104 registered cases of this type, the SHARE Foundation recorded 91 such cases in 2016. However, it seems that various types of exerting pressure and threats against journalists and activists remain relatively high as much as in previous years due to impunity.

Legal uncertainty is the main effect of threats to digital rights and internet freedom, which means that perpetrators were never identified nor prosecuted. Furthermore, despite the decline of technical attacks, there is a clear need for advancing defense capacities in the local cyber sphere. One of the key conditions of online security in general population certainly is the systemic improvement of digital literacy.

It should be noted that in cyberspace the defense is usually more expensive than the attack, which is discouraging for small and independent online and citizen media who cannot afford cyber security experts nor technical solutions for their protection. The decline in the number of serious technical attacks does not mean that defense resources should not be constantly improved. However, acquiring higher levels of digital security often involves complex procedures and changes in daily habits, which may decrease the efficiency of journalists and organizations.

The attacks and threats aimed at journalists and bloggers because of what they wrote, produce a chilling effect[24] that spreads through the entire online community, in Serbia supposedly amounting to around 60 of the population. Therefore, it could be said that citizens do not feel empowered and protected in the digital environment, which may add to other factors impeding the development of an information society and wider use of digital technologies.

Authorities' technical and organizational capacities for an adequate reaction in each of the cases are indeed limited. However, there is a growing disparity in the selection of incidents that get full and efficient attention of the police, prosecutors and courts. Processing of cases involving cyber attacks and threats to online media, investigative reporters and citizen media that express dissenting views, is becoming extremely inefficient in some cases. Such practice reduces the trust that citizens and online media organizations have in legal protection by authorities who should assume a more active role in securing human rights and freedoms online.

1.3.2. MONITORING RIGHTS AND FREEDOMS ONLINE – SELECTED CASES

From the traditional media perspective, the internet is as public space often associated with the lack of responsibility and various types of violation of rights, abetted by offenders' anonymity. On the other hand, the incidents testing the boundaries between the private and the public, threats to freedom of individuals that face disproportionate power of global corporations and state institutions, or digital tools that refined techniques for manipulating public opinion beyond imagination, are just some of the pressing issues which public policies, and the entire community, need to address. The five selected cases processed in 2016 may serve as an example of new challenges for freedom of expression online.

1. YOUTUBE AGAINST OMBUDSMAN

The question of influence that online platforms exercise through the control of content posted by users was raised in Serbia in August 2016 when Serbian Ombudsman's YouTube channel was suspended. Rarely used and only for reposting segments of TV shows and news reports on cases the Ombudsman's office was involved with, the channel was apparently suspended by YT moderators as a result of other users' reports. The popular video sharing platform refused the appeal request filed by the Ombudsman's associates, while in the meantime the email used for uploading the video clips was also blocked. In the end, access to the YT channel was enabled but without any explanation or clarification. [25]

[24] "In a legal context, a chilling effect is the inhibition or discouragement of the legitimate exercise of natural and legal rights by the threat of legal sanction" (Wikipedia); "Is online freedom in danger?", SHARE Foundation [in Serbian] http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-forumasa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

With the help of the European Digital Rights association (EDRi), the SHARE Foundation contacted the Google policy team in Brussels, asking for the explanation of the video platform's policies on suspension and reactivation. According to their representative's claims, videos and channels are not automatically removed from YouTube, no matter how often they are flagged. As stated in their response, reports of content are not reviewed by machines but by a team of humans who deal with each report individually. Users should receive notifications during both suspension and reinstatement, while the lack of the latter in the Ombudsman's case was deemed an honest mistake.

Considering the sheer amount of content, the described procedure of YouTube moderation seems hard to conduct, nevertheless remaining insufficiently transparent. The problem of algorithmic censors and mechanical management of public sphere through selection of available content, is a growing problem on a wider scale.

2. THREE YEARS TO ACQUITTING VERDICT FOR FORUM USERS

At the end of March 2016 Ognjen Rasuo, the defense attorney for three members of "Parapsihopatologija" forum, announced on Twitter that the forum users had been finally acquitted of charges of threatening and endangering the safety of a film director, Boris Malagurski.[26] The trial opened against the forum users on account of statements posted at a non-public section of the forum, and stretched over three years until it was finally closed by the Supreme Court of Cassation ruling that cleared forum members Rastislav Dinic, Marko Nikolic, and Nemanja Paleksic of all charges. Despite the unjustifiably long process, the final decision in favor of the forum users seems important for freedom of speech online, at least alleviating to some extent the chilling effect that discourages netizens to express their views freely, not fearing potential legal ramifications.[27]

Criminal proceedings were initiated on account of statements made in a forum discussion on Boris Malagurski's documentary, "The Presumption of Justice", conducted within a section available only to registered forum members. In the movie, filmed several years after the murder of a French football fan Brice Taton in Belgrade in 2009, the author depicts the events as an accident and claims that the course of the subsequent investigation

[25] "How social media manage public space: YouTube against Ombudsman", SHARE Foundation, 2016. [in Serbian] http://www.shareconference.net/sh/defense/kako-mreze-ureduju-javni-prostor-youtube-protiv-ombudsmana

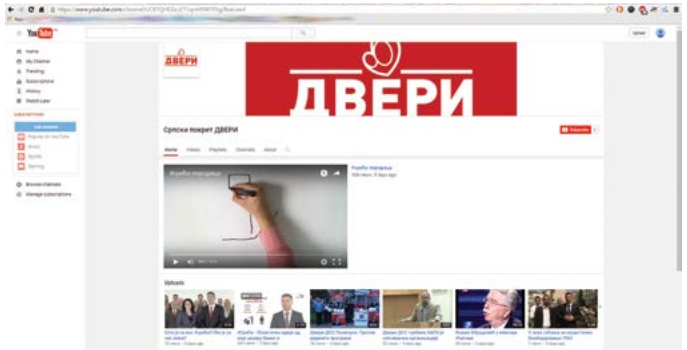
[26] Laywer's tweet: "The Supreme Court of Cassation overturned the verdict in the case Malagurski v. PPP. Forum members free. :)" [in Serbian] https://twitter.com/ORasuo/status/715538553141379073

[27] "The chilling effect of convicting verdict in Malagurski case – is freedom of speech online endangered?", SHARE Foundation, 2014. [in Serbian] http://www.shareconference.net/sh/blog/ciling-efekat-presude-protiv-dva-forumasa-u-slucaju-malagurski-da-li-je-sloboda-izrazavanja-na

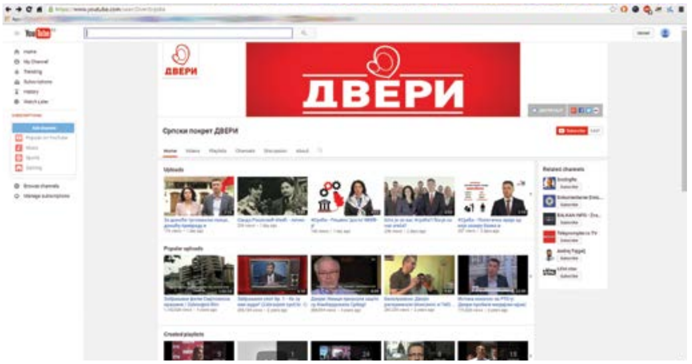
and trial was the result of political pressure. The forum users' comments were vulgar and offensive, and the author perceived them as a threat to his safety. The trial court's ruling found the forum users guilty, but was reversed by the Court of Appeal because of several procedural errors.[28] The forum users were again convicted on retrial, but the ensuing appellate decision changed the legal qualification of the offense and reduced the sentence. The Supreme Court of Cassation, finally, ruled that in this case "the law which cannot be applied was applied", acquitting the defendants.[29]

3. FALSE "DVERI" CHANNEL

A series of promotional video clips, allegedly produced by the right-wing movement "Dveri", appeared on YouTube during the parliamentary elections in 2016. The contested clips discredited the movement and its leaders by ascribing them ideas purportedly different from their original policies, presenting the content as their own (for example, a video dedicated to March 8 was gravely insulting to women).[30] By the beginning of April, at the peak of the campaign, a YouTube channel, visually similar to that of "Dveri", was set up in order to distribute the clips.



The false channel of the Dveri political movement



Official channel of the Dveri political movement

[28] "Training the public with fear", October 2014 [in Serbian] http://www.autonomija.info/milica-jovanovic-vaspitavanje-javnosti-strahom.html

[29] The Supreme Court of Cassation ruling Kzz 1203/2015 [in Serbian] http://www.vk.sud.rs/sr/кзз-12032015

[30] Reports on video clips in tabloids: [in Serbian] http://informer.rs/vesti/izbori/65644/VIDEO-NEVIDJENA-PREDIZBORNA-BRUKA-Dveri-otcepili-Kosovo-Metohiju-Srbije, http://www.alo.rs/u-dverima-ovako-tretiraju-zene-video/38613

It is worth noting, however, that during the campaign the "Dveri" movement largely turned to the internet and free sharing platforms that, alongside "Dosta je bilo" movement, practically made them pioneers in applying free online resources for political propaganda in Serbia. Despite the initial prognosis and poor representation in traditional media, both movements managed to win seats in the Parliament.[31]

4. TWITTER ACCOUNT SUSPENSIONS

The managing editor of the weekly magazine "NIN", Nikola Tomic, was shut out from access to his Twitter account @N _ Tomic in June 2016.[32] Suspicions that the account was hacked were not established, but instead it turned out it was a suspension based on "a suspicious activity" as the automated reply stated. The suspension coincided with the magazine's report on political responsibility of Serbia's minister of interior affairs for covert demolishing of buildings in Belgrade,[33] because of which the minister later filed a lawsuit.

In this case it was not possible to carry out technical analysis, nor it could be established which mechanism of the popular microblogging platform was used for suspension due to security reasons. Whether for attempted takeover of the account, users' fake reports, or something else, the lockdown procedures are usually fully automated, and the suspension lasts until the real owner unlocks the account.

Complex, different passwords for different accounts on social media and emails, occasional changes of passwords and their safe keeping, are the basic recommendations for protecting the integrity of personal accounts.

5. DR. TATJANA MRAOVIC AGAINST BLOGGER "VITKI GURMAN"

Legal actions against authors of blogs are still a rare occasion in Serbia, while one of the first court cases took place when Dr. Tatjana Mraovic filed a private criminal complaint for libel against Maja Petrovic, who runs a healthy diet blog "Slender gourmet".[34]The matter of complaint was an article published in 2015 in which the blogger criticized the promotion of margarine as a healthy food ingredient.[35] The first instance verdict acquitted Maja Petrovic of libel, and Dr. Mraovic was ordered to reimburse the blogger with the costs of the proceedings. As the plaintiff appealed the verdict, the procedure is still open.

[31] Analysis of online and social media during 2016 election campaign in Serbia, SHARE Lab, 2016. [in Serbian] https://labs.rs/sr/analiza-onlajn-medija-i-drustvenih-mreza-tokom-izbora-2016-u-srbiji/

[32] Tweet: "...until the reputable @twitter reinstates access to the hacked @n _ tomic. Share away!" [in Serbian] https://twitter.com/blablaTomiccc/status/745206034235555840?ref _ src=twsrc 5Etfw

[33] Tweet: "How Nebojsa Stefanovic unseated his best police inspector" [in Serbian] https://twitter.com/N _ Tomic/status/743763398702182400/photo/1?ref _ src=twsrc 5Etfw

[34] Slender gourmet in court [in Serbian] http://vitkigurman.com/vitki-gurman-na-sudu/

[35] Shameful teamwork – "Dijamant" company and Dr Tatjana Mraovic [in Serbian] http://vitkigurman.com/tatjana-mraovic-doktorka-za-margarin/

At the time of publishing the text about "the margarine doctor", the blogger's reputation was targeted[36] and then her blog's hosting provider received a request to prevent access to the blog due to "hate speech" and "violations of the basic rules of behavior on the Internet." [37]

1.3.3. ALGORITHMIC CONTENT MANAGEMENT

Quantities of information published on the Internet require special mechanisms for content management and distribution to the targeted audience. As Internet users spend more and more time on platforms mediating content sharing between creators and consumers (Google, Facebook, and YouTube are the three most popular Internet services in Serbia), distribution mechanisms gain more and more attention in the local digital media sphere.

Whether a media outlet, an organization, or an individual appear as creators or distributors of content via a platform, the content passes through a variety of obstacles and filters on its way to the desired audience. Platforms mostly manage the distribution process with the help of automated mechanisms based on mathematical algorithms, and occasionally using human judgment of the staff involved in the process.

The life cycle of online content begins by upload on a particular platform, triggering an automated check-up through an "upload" filter. Each platform may have a different set of checkups, depending on the technology used and the established policies on illegal and harmful content but, in principle, those filters are threefold:

1. Filtering of content that was already marked as unauthorized and harmful, by comparing the hash values[38] and keywords (terrorism, hate speech, child pornography, etc.).
2. Filtering "spam"[39] by comparing the hash value and analysis of distribution channels.
3. Filtering of content through visual, video and audio recognition, based on the catalog of works protected by copyright.

If an internal identification or checkup system marks content as illicit, the platform either automatically prevents the publication or removes the content after it was published. In certain cases (copyright) reinstating the content can be enabled based on subsequent consent of the copyright holder. It is worth noticing that administrators of certain types of communication channels, within the community they administer, can impose additional types of filtration (according to predefined keywords and a catalog of vulgar expressions).[40] Bearing in mind that this type of content management is not flexible enough to take into account all the standards of freedom of expression, with rigid automated decision-making, violations of freedom of speech and freedom of information are not rare.[41]Nevertheless, the algorithm enables that instead of removal, content gets labelled as not suitable for a specific group of users (children, young people, sensitive consumers, etc.).

If the content passes the filters during the upload to a platform, it is still not certain whether and to what extent it would be accessible to the desired audience. Various factors affect the decision as to what type of content will be automatically displayed to individual users, the list not being final:

- Type of person that distributes content (user, page, group, company, etc.);
- Content format (text, video, audio, photo, etc.);
- Content relevance for platform users;
- Automatically generated user profile;
- User requests (hide, star, always display, etc.);
- Specific relationships between content and users (tagging, etc.);
- Boosting, a form of online promotion, or sponsoring content.

So it turns out that not all actors, all types of content, and all users within the digital media sphere hold an equal position. Platforms that host a lot of content (Facebook, YouTube, and others), implement editorial design of content that is available to users with the help of automatic processing.

Once the content becomes available to users - through automatic displays, as a search result, or by direct access to communication channels (profiles, channels, pages, groups, etc.) – the content is further checked through the system of reporting or flagging in accordance with community policies (guidelines, terms of use, etc.). All interested parties may submit a report of unauthorized and harmful content, which would initiate a procedure for examining the merits of the application and enforcing possible sanctions. The basis of a report is reviewed by human teams engaged by the platform, but there is a growing need for this process to be run by expert organizations.[42] Upon accepting a report of the illicit content, the possible sanctions include removal of the content itself as well as temporary

[36] "Woke up this morning to discover..." [in Serbian] https://www.facebook.com/VitkiGurman/posts/759608117477916?hc _ location=ufi 20htt

[37] "How little Johnny imagines the Internet" [in Serbian] https://www.facebook.com/notes/sibin-gra C5 A1i C4 87/kako-mali-perica-zami C5 A1lja-internet/10153795172603092

[38] A one-way, irreversible function used to transform data of unlimited size into a numeric value of a fixed length.

[40] Example: https://www.facebook.com/help/131671940241729?helpref=related

[41] Examples [in Serbian]: Parody and copyright: let's defend remix culture! http://www.shareconference.net/sh/defense/parodija-i-autorska-prava-odbranimo-remiks-kulturu; The way social media manage public space: YouTube v. Ombudsman http://www.shareconference.net/sh/defense/kako-mreze-ureduju-javni-prostor-youtube-protiv-ombudsmana; Monitoring of 2017 presidential online campaign https://labs.rs/sr/izbori2017/

[42] A good example is the German nonprofit investigative newsroom Correctiv, engaged to prevent spread of fake news via Facebook in German-speaking areas https://correctiv.org/en/correctiv/

or permanent suspension of the account used for distribution of content. Experts are of the opinion that the content management mechanisms triggered by user reports are not transparent enough, both in terms of the process and in terms of criteria applied for establishing a balance between freedom of expression and conflicting values, while "legal remedies" are insufficiently developed.

Furthermore, there are particular types of content removal resulting from the cooperation of a platform with authorities and international content management organizations. Most commonly, platforms enable removal of content based on national court decisions or in response to reports of specialized organizations that protect the interests of certain categories of population, such as the EU Agency for Network and Information Security. [43]

1.4. EU INTEGRATION

RECOMMENDATIONS

To urgently draft a new Personal Data Protection Law, as planned by the Action Plan for Chapter 23, and in line with the new EU General Data Protection Regulation and the newly proposed Model for Personal Data Protection Law by the Commissioner for information of public importance and personal data protection. The implementation of the measures from the Action Plan for Chapter 24 includes capacity building in the area of high technology crime, whereby the new systematization of workplaces within the Ministry of Interior Affairs has been identified as a significant obstacle, more specifically its high-tech sector at both the operational level and the level of communication with international bodies (Interpol, Europol, Eurojust, etc.).

[43] ENISA https://www.enisa.europa.eu/about-enisa

1.4.1. CHAPTER 23

Two key chapters for Serbia's accession negotiations with the European Union, Chapters 23 and 24, were opened in July 2016. The Action Plan for Negotiation of Chapter 23, regarding judiciary and fundamental rights, was adopted at Serbia's Government session on 27 April, 2016. [44]

The SHARE Foundation is particularly interested in the segment of this process that addresses personal data protection, outlined in the Action Plan as the constitutional and legislative compliance with the EU legal framework. The document emphasizes that EU regulations in this area are subject to reform and that Serbia will align its legislation after new regulation is adopted. It also states that a new law on personal data protection will be introduced in accordance with the tables of compliance with the existing EU acquis, the new EU General Data Protection Regulation passed in May 2016, and the Law Model proposed by the Commissioner.

The date set for adoption of a new law expired at the end of 2016, while the fourth quarter of 2017 was set as the deadline for subordinate legislation. Since the new law was not adopted according to plan, the bylaws are expected to be pushed to a later date as well.

A significant measure proposed by the Action Plan refers to strengthening human and financial resources of the Commissioner for information of public importance and personal data protection. As defined, the analysis of the Commissioner's needs would be carried out during the first and second quarters of 2017, so that by 2019 the number of employees will gradually increase from the current number of 64 employees, to the final target of 94 employees.

Upon adoption of the EU General Data Protection Regulation, the Action Plan emphasized it would be necessary to make appropriate changes regarding the Commissioner's authority, as well as to develop a new rulebook on internal organization and systematization of workplaces.

1.4.2. CHAPTER 24

The screening report for Chapter 24[45], as well as the European Commission Progress Reports for Serbia from 2013 and 2014, all point to the fact that the fight against cyber crime in Serbia is still in its initial phase. The Progress Report issued in 2016 obliged Serbia to adopt a strategy on high-tech crime. The screening report acknowledged that Serbia: established a special anti-high-tech crime department at the Ministry of Interior Affairs, and the Special Prosecutor's Office for Fight Against High-Tech

[44] Action plan for Chapter 23, Ministry of Justice http://www.mpravde.gov.rs/files/Action%20plan%20Ch%2023.pdf

[45] Screening report Serbia Chapter 24 - Justice, freedom and security, Delegation of the EU to the Republic of Serbia http://www.europa.rs/upload/2014/Screening-report-chapter-24-serbia.pdf

Crime; confirmed the Council of Europe's Convention on High-Tech Crime ("Official Gazette of RS", no. 19/2009); largely harmonized the provisions of Directive 2013/40 / EU on attacks against information systems. It is concluded that it is necessary that Serbia adopts amendments to its existing regulation, particularly in regard to the prescribed legal sanctions, in order to comply fully with the EU legal framework in the area of cyber crime. In post-screening recommendations, the Commission has determined that it is necessary to ensure the continuation of specialized training, as well as to enhance the capacity of law enforcement agencies engaged in fighting cyber crime.

The action plan for Chapter 24 recommends a series of improvement measures:

1. Provide further specialized training and enhance the capacity of law enforcement agencies to counter cyber crime:
   - - Draft a proposal of relevant bylaws to improve organizational, personnel, and technical capacities for curbing cyber crime.
   - - Strengthen the capacities of the Special Prosecutor's High-Tech Crime Office.
   - - Strengthen the capacities of the Special Prosecutor's High-Tech Crime Office, Special Police High-Tech Crime Department, courts, and other relevant institutions through training.
   - - Establish a specialized investigation unit for credit card abuse, internet trade and electronic banking, within the Ministry of Interior Affairs - departments for organized crime and for the high-tech crime.
   - - Establish a specialized unit for control of illicit and harmful content on the Internet, within the Ministry of Interior Affairs - departments for organized crime and for high-tech crime (this unit would also investigate child pornography through an automated support system – a computer system for analysis of photo and video material that contains child pornography).

2. Harmonization of Serbian laws with the legal framework of Directive 2013/40 and EU standards in the field of cyber crime.
   - - Analyze the current legislative framework to determine the level of compliance with the EU acquis and standards.
   - - Draft a law and subordinate acts based on the conducted analysis.

3. Strengthen cooperation between state authorities and civil society organizations in the area of cyber crime.

4. Develop and sign agreements on cooperation between state authorities and civil society organizations in fighting cyber crime.

In its Progress Reports from 2013 and 2014, the European Commission has acknowledged Serbia's efforts to combat cyber crime through improving cooperation with the State Prosecutor's Office, and organizing training for police officers and senior executives, including training on national level investigations and in cooperation with other countries. However, the Commission warned of the need for structured training and adequate resources. Namely, there is a need to strengthen the capacity of the Department for Combating High Technology Crime at the Ministry of Interior Affairs, in order to better manage investigation of the growing range of complex criminal activities, as well as the need to introduce specialized techniques to align the Department with contemporary international operational standards. In its recommendations, the Commission also recognized the need to establish close cooperation of private and public sectors and the academic community. Thus, additional specialized training, better coordination between institutions and an adequate budget are needed for a comprehensive fight against cyber crime in Serbia.

2. FREEDOM OF SPEECH

RECOMMENDATIONS

To empower self-regulatory bodies and mechanisms; to establish models of reputable media systems (a mark of trust, ethical conduct online); to test and analyze facts (fact-checking); to promote benefits of media registration, as well as those of digital literacy of children and youth, and general public for online and citizen media; to incorporate provisions on mandatory identification of registered online media through authentication within the future law on electronic documents, electronic identification and trust services for electronic transactions.

2.1. ONLINE MEDIA IN SERBIA

2.1.1. DEFINITION AND LEGAL PROTECTION OF JOURNALISTS

Given the environment in which the very presence enables participation in production and distribution of information, online and citizen media are particularly hit by demands for introducing some sort of licensing or formal regulation of the "right" to be a journalist. In that sense, the Internet is often referred to as an ecosystem in which no rules of good journalism exist and where "everyone can write whatever they want" - with an equal chance of influencing public opinion like the educated, editorially shaped journalism that complies with legal and ethical standards. Apart from the context of self-regulatory mechanisms, this issue is particularly raised with regard to the two special forms of legal protection of journalists: the confidentiality of sources and the protection of journalists' safety. Furthermore, citizen journalists may face discrimination concerning equal access to information, especially in communication with public authorities that may treat professional and citizen journalists differently.

It appears that Serbian courts assign these two special rights only to professional journalists, i.e. members of professional associations or those hired by formally registered media. However, in view of the dramatic changes within the media environment in recent years, considerable attention has to be paid to aligning the standards of prosecution and court practice with the principle stating that special legal protection belongs to all participants in public communication who have no formal journalist status, but performs a journalistic act on a regular or occasional basis, informing the public on issues of common interest.

If a new definition of media and journalists is needed, the Recommendations of the EU Committee of Ministers would be a good basis. Also, a 2012 report by the former UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression Frank La Rue, defines journalists as "individuals who observe and describe events, document and analyze events, statements, policies, and any propositions that can affect society, with the purpose of systematizing such information and gathering of facts and analyses to inform sectors of society or society as a whole."

Good practice suggests that this question can be answered with regard to two aspects - status and action. Namely, citizens and organizations can gain special rights either through a professional relationship with a media organization, press association, and self-regulating instruments; or through performing a journalistic act that is, collecting and disseminating information in common interest and exercising control over private or public power within a society.

In cases where a functional link can be established, special privileges of a journalist or a media organization are presumed; on the other hand, in the case of a contextual relation, it seems that it is upon a citizen to prove to be performing a journalistic act on a particular occasion, entailing the benefits of a journalist.

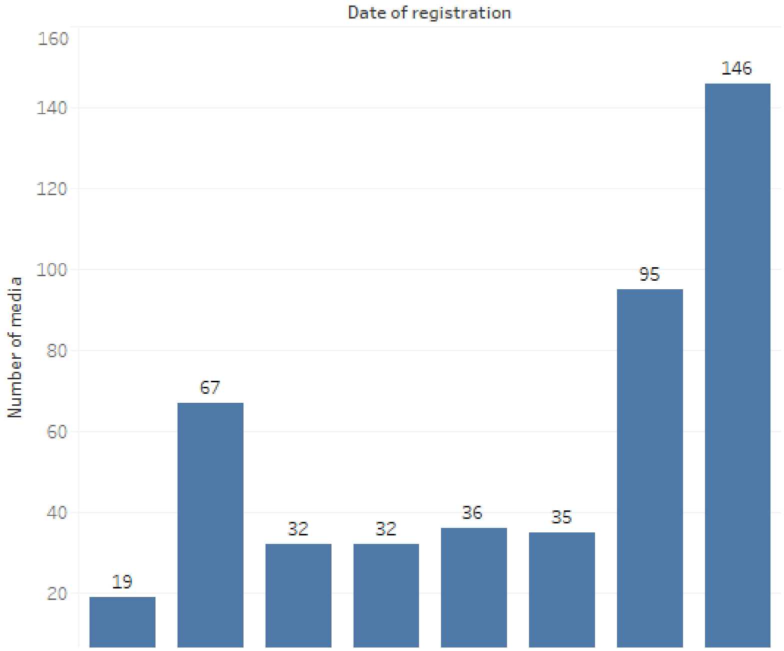
Resolving a number of important issues may serve as possible points of reference for future (self-)regulatory models that go beyond the framework of sectorial rules: At which point does an individual or an organization begin their professional media engagement and how does it affect their regulatory status? Does it make sense to regulate small media of insignificant market power? What is the appropriate criterion for potential regulation of a large media organization with strong influence on certain social groups, and significant profits? Is there a need for automatic application of media regulation in case of an unregistered online media outlet? At which point are the rules of advertising and consumer protection be activated?

2.1.2. MEDIA REGISTER STATISTICS

Since the introduction of the Media Register at the Business Registers Agency (previously: the Public Media Register), until the end of February 2017, 539 online media have applied for registration, out of which only 14 submitted a request for deletion.

The number of registered online media has been growing steadily over the last three years: in 2014 there were 35 online media registered, with numbers of the newly registered increasing to 95 in the following year, while in 2016 there were 146 registered online media. This trend can be explained by the adoption of a new Law on Public Information and Media that does not prescribe mandatory registration, but rather treats the Register entry as a prerequisite, among else, to co-financing projects from public sources.[49]

If we take a look at the period before the adoption of new media laws, the biggest leap in the number of newly registered media was recorded in 2015 (more than twice the number compared to the previous year). The growth slowed down in 2016.

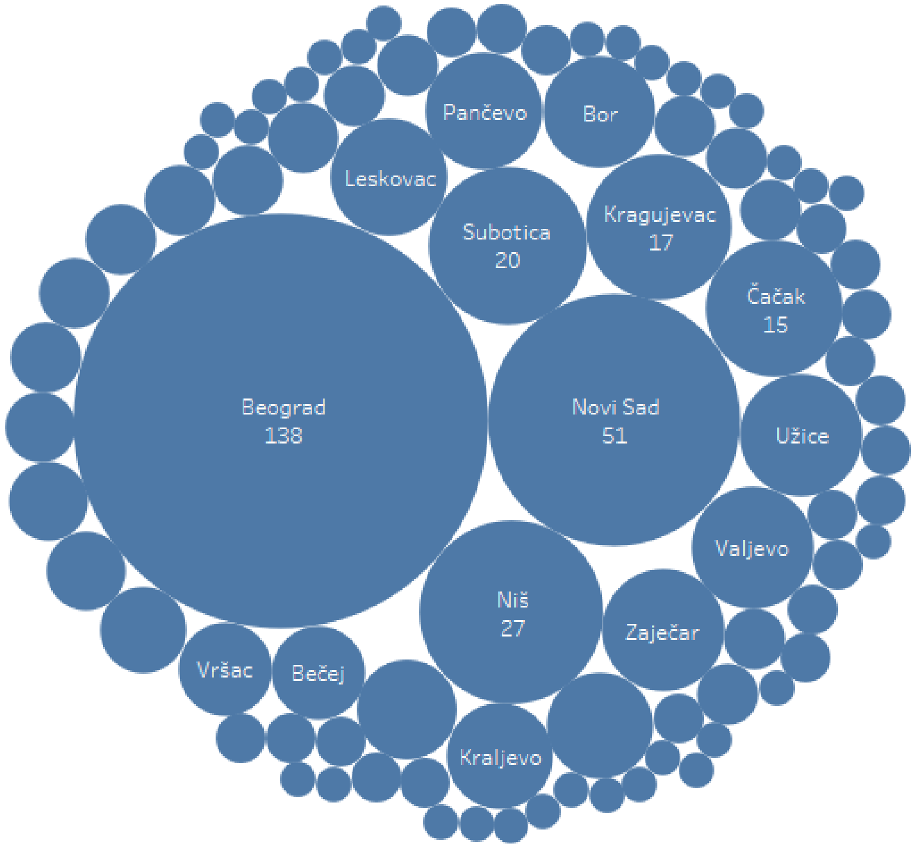


The number of registered online media per year

When it comes to the number of registered online media, major cities such as Belgrade (132), Novi Sad (49), and Nis (25), as well as regional centers (Kragujevac, Zajecar, Subotica, Cacak), expectedly lead the table.

In the first two months of 2017, a total of 65 new online media were added to the Register, confirming a trend of growth.

An interesting insight into the behavior in the online media environment is provided in the Share Labs research conducted during the 2016 election campaign, which analyzed the relevant content of a dozen most influential domestic news portals; although it should be noted that elections are a sort of an extraordinary event within a society, when behavior may significantly differ.[50] According to this research, the average "life expectancy" of a piece of news in Serbian online media is between one and two hours.



The number of registered media per city

During the first two hours the news gets commented on the web page and shared around social networks, only to get lost under the wave of new content. Fast production pace is dictated by the three largest news agencies in Serbia (Tanjug, Beta, FoNet), who produce more than 60% of content published by online media. The original content of online media accounted for only one quarter of texts covering the election campaign.

Social networks presence varies across traditional and online media: from one-way communication through mere posting of new content links, to full use of particular platform options for delivering a variety of content, encouraging two-way communication and more audience engagement. Differences in the use of social media platforms are obvious from the number of followers any given media gathered over time. The public TV broadcaster's Facebook page has only 8,000 likes, whereas the same media outlet attracted over 80,000 followers on Twitter. On the other hand, the online investigative news portal KRIK has attracted almost four times more engaged users on Facebook than on Twitter.

For most traditional media Facebook is the primary channel for distribution of content: hundreds of thousands of likes confirm this on FB pages of daily newspapers such as Politika (109,000), Vecernje Novosti (356,000), Kurir (748,000) or Blic (892,000), as well as Novi Sad Radio 021 (126,000),

[49] Law on Public Information and Media, Official Gazette of RS, no. 83/2014, 58/2015 and 12/2016 [in Serbian] http://www.paragraf.rs/propisi/zakon _ o _ javnom _ informisanju _ i _ medijima.html

[50] Online and social media analysis in the 2016 elections in Serbia; SHARE Labs, 2016 [in Serbian] https://labs.rs/sr/analiza-onlajn-medija-i-drustvenih-mreza-tokom-izbora-2016-u-srbiji/

TV Pink (341,000), or TV B92 (499,000). Compared to Twitter, Blic has half as many followers as on Facebook, while TV Pink has up to fifty times less (6,000).

2.1.3. THE LEGAL POSITION OF ONLINE MEDIA

The Law on Public Information and Media[51] defines the media and the conditions under which an organization is legally treated (Articles 29-31). The definition includes electronic editions of traditional media (press, agencies, radio and TV stations) and independent electronic editions, or editorially shaped websites or internet portals, provided they are registered in the Media Register. The Law clearly excludes internet forums, social networks and similar platforms, while other forms of production and distribution of information on the Internet (blogs, web presentations, online portals) are not considered media unless they are registered in the Media Register.

Thus, the legislator has left the choice to the citizen and online media to register, if they wish to gain the legal status with all the rights and obligations. Unregistered citizen and online media remain outside the scope of this Law.

Such approach limits the access to special forms of legal protection and other privileges enjoyed by the media, on the grounds of formal registration. On the other hand, unregistered online and citizen media are not obliged to comply with provisions prescribed by the media law.

Responsibilities of registered media include, among else, due diligence, the expanded accountability of editors, journalists and publishers, and the transparency of ownership. The registered media status provides protection of sources, an undisputed regimen of legal protection for journalists, extraordinary basis for exemption from criminal liability, as well as more direct access to information and events, special copyright exemptions, and access to public funds allocated for projects concerning general dissemination of information.[52]

Registered media are obliged to have a permanently available impressum, containing their name, publisher's address, editors' names and the like. The content that media publish fall under rules regulating media discourse, such as the prohibition of discrimination or hate speech. Media content must also not harm the moral, intellectual, emotional, or social development of minors. In other words, it is an aggravating circumstance if an online offense is committed by a registered media organization.

[51] Law on Public Information and Media [in Serbian] http://www.paragraf.rs/propisi/zakon _ o _ javnom _ informisanju _ i _ medijima.html

[52] N. Krivokapic, O. Colic, M. Maksimovic, Legal status of online media in Serbia: A guide for online and citizen media as users, SHARE Foundation, 2015. [in Serbian] http://www.shareconference.net/sites/default/files/u742/vodic-pravnipolozaj _ onlajn _ medija _ u _ srbiji _ - _ preview _ .pdf

The Media Register is run by the Business Registers Agency.[53] The registration process requires the media to have a publisher (legal entity or entrepreneur, registered for the work in the particular industry), an editor-in-chief, verified information about the natural and legal persons who directly or indirectly hold more than 5% of the share capital of the publisher registering the media, and so on. The registration fee is 2,800 RSD, which is around 10% of the minimum net wage in January 2017.

PADVANTAGES OF A REGISTERED MEDIA OUTLET

- Protection of sources
- Special regimen of legal protection
- of a journalist's personal integrity
- Special grounds for criminal prosecution exemption
- Access to information and reporting accreditation
- Access to public funds –
- co-financing projects in the field of public information in public interest
- Special rules on free use of copyrighted work for media

RESPONSIBILITIES OF A REGISTERED MEDIA OUTLET

- Due diligence – "accountable journalism"
- Extended liability of editors, journalists and publishers
- Rules concerning information taken over from other sources
- Other special rules: impressum, ads, copyright, etc.
- Mandatory reports of funds received from public sources

[53] About the Media Register, SBRA http://www.apr.gov.rs/eng/Registers/Media/AboutRegister.aspx

RECOMMENDATIONS

To enhance the rules of running the Media Register in regards to more detailed collected data, the extent of their public availability, defined mechanisms of regular information update, and prescribed sanctions. To secure that data and metadata from the Media Register are available for reuse, free of charge, in an open, machine-readable data format. To enable the creation of a register of audio-visual media services provided online and audio-visual services on demand.

2.2. MEDIA STRATEGY 2011-2016

The Strategy for the Development of the Public Information System in the Republic of Serbia by 2016 was passed in the autumn of 2011, marking the start of a new reform cycle in the media sphere.[54] The primary aim of the Strategy was the withdrawal of the state from ownership in the media, as well as the transparency of media ownership, new models of financing media from public funds, and the like, in accordance with the proclaimed principle of preventing the influence of public authorities on the media. Focused on public TV broadcasters (national RTS, and regional RTV) and the local media founded by the local authorities, the Strategy paved the way for a new set of media laws adopted three years later, regulating the related areas more closely.

Given the urgency of withdrawal of the state from media ownership, the Strategy had neglected a number of issues emerging from the already then apparent radical changes in the production and distribution of information in the digital environment. The document dealt in more detail only with the digitization of the television signal, which was completed in 2015.

In its second chapter the Strategy distinguished traditional electronic media from those that distribute content on the Internet, noting the lack of regulation in this area. The document expressed the intention of the state to encourage technological innovation in the media sphere and the development of new media platforms. However, it did not provide any guidance in relation to future regulatory or incentive models, apart from stating the obligation to treat media content of public interest produced on new technology platforms equally when considering projects for financial support from public sources.

The Strategy recalled the Digital Agenda for Europe that promotes fast and ultra fast Internet access for all, and the appropriate development of broadband services. Finally, the Strategy confirmed that the state of Serbia "recognizes the Internet as a fundamental human right, as common good open and easily accessible to all, in line with the freedom of expression and information", which is a key political decision to insist on in future documents of this kind, and to take into account when drafting further relevant regulations.

The set of new media laws was passed by the Parliament of Serbia on 2 August 2014, enabling the state to withdraw from media ownership over the next year, switch to project financing, and transform the regulatory body for electronic media. The Law on Public Information and Media, the Law on Electronic Media and the Law on Public Media Services came into force ten days later. All three laws were subject to subsequent amendments.

Although it was expected that the work on the new media strategy would begin even before the old one formally expired, no official announcement was made. Several groups from the media community, along with civil society organizations have independently launched a series of public debates at the end of 2016 in an effort to articulate some of the key issues that should be addressed in the new strategic document.[55]The need for digital literacy of the media and the public has been recognized in the course of this dialogue as one of the most important issues for the future strategy, as well as a more precise definition of government position concerning online media.[56]

By late March 2017, Serbia's Government adopted the amendments[57] of the bylaw regulating the transfer of capital without remuneration of media employees, originally intended for addressing occasions in which a publicly owned media organization has not been privatized by the legally prescribed deadline. The two journalists' associations, the Independent Journalists' Association of Serbia (NUNS) and the Independent Journalists' Association of Vojvodina (NDNV), have warned that this enables transfer of media ownership back to local government, which is in collision with media laws, signaling that the state "has definitely given up on media reform and announced the reetatization of the media."[58]

[54] Strategy for the Development of the Public Information System [in Serbian] http://nuns.rs/reforma-javnog-informisanja/strategija.html

[55] Conference from the SpeakUp! series, "Towards a modern media policy", TACSO and OSCE, November 2016. [in Serbian] http://www.tacso.org/news/events/?id=14590

[56] Conference from the SpeakUp! series, "Towards a modern media policy", TACSO and OSCE, November 2016. [in Serbian] http://www.tacso.org/news/events/?id=14590

[56] A series of debates on the new media strategy was also organized by Novi Magazin with the support of the Open Society Fund [in Serbian] http://www.novimagazin.rs/vesti/onlajn-informisanje-digitalna-prava-i-vestine-medijska-pismenost-brzi-razvoj-brzi-i-problemi

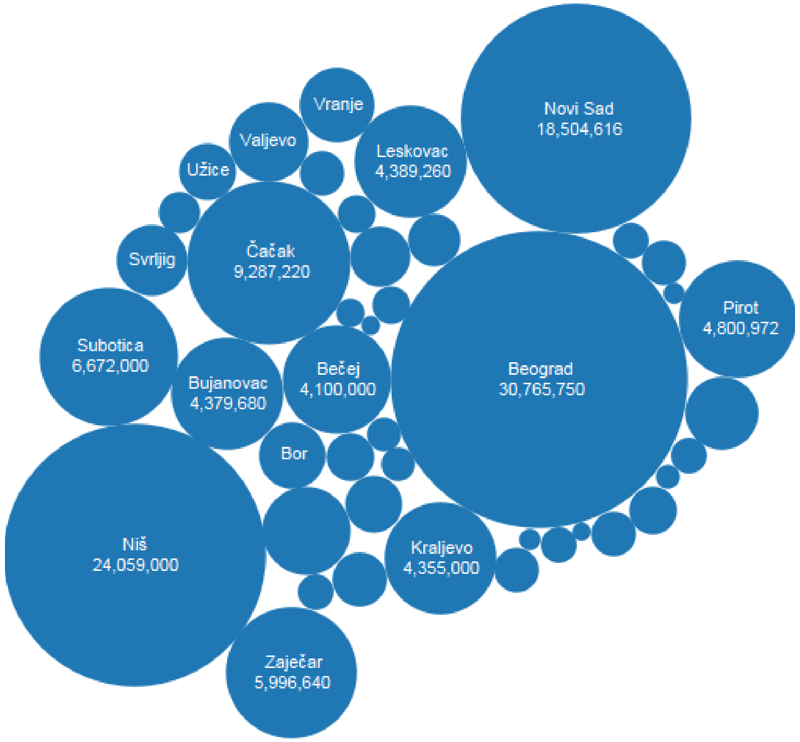
[57] Bylaw amending the bylaw [in Serbian] http://www.srbija.gov.rs/extfile/sr/289619/uredba-prenos-kapitala-zaposleni-mediji046 _ cyr.zip

[58] NUNS and NDNV: The state becomes the media owner again [in Serbian] http://nuns.rs/info/statements/30565/nuns-i-ndnv-drzava-ponovo-postaje-vlasnik-medija.html

The ministry in charge dismissed the allegations, stating that the amendments to the bylaw prevented the media in which privatization was cancelled to be shut down, which would happen through by bankruptcy or liquidation: "The Ministry of Culture and Information assures NUNS and NDNV that it has not given up on the media reform. On the contrary, in this way, we only want to protect the right of citizens to be informed and to provide the opportunity for journalists and media workers to continue working in public interest." [59]

2.3. IMPLEMENTATION OF MEDIA LAWS: PROJECT FINANCING

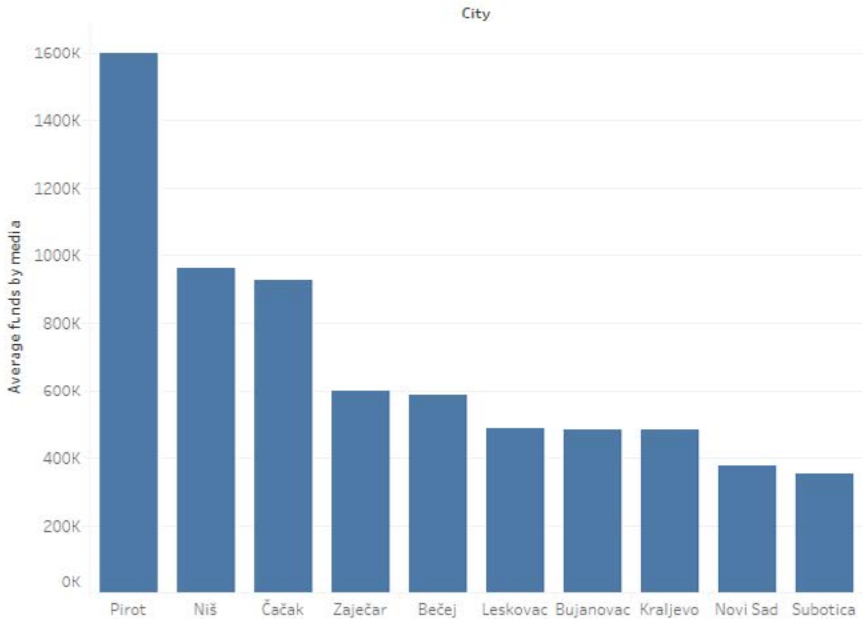
According to the data available in the Media Register at the Business Registers Agency, which includes data on public funding at national, regional and local levels, budget allocations are directed to cities where registered online media are mostly located. In sum, most public funding goes to online media in the largest cities (Belgrade, Nis, Novi Sad), and to the towns towards which different regions gravitate (Zajecar, Cacak, Bujanovac. Subotica).



Allocated funds for online media per city (RSD)

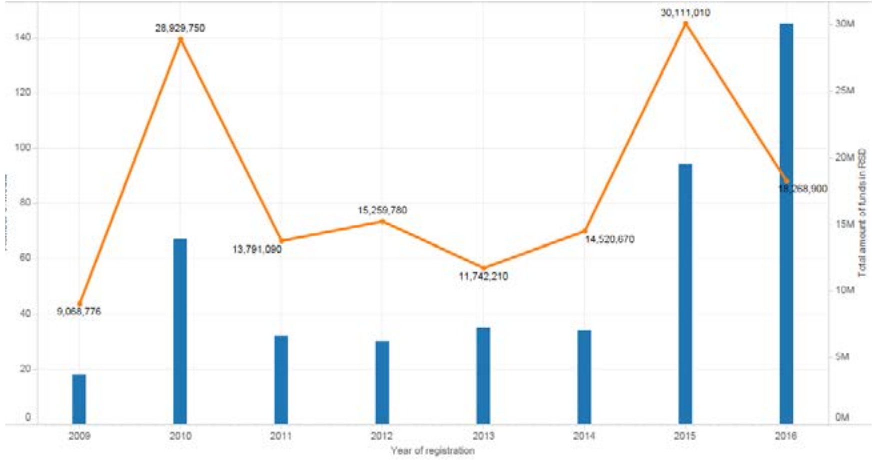
[59] Ministry of Culture and Information: NUNS and NDNV for termination, Government for survival of the media [in Serbian] http://www.kultura.gov.rs/lat/aktuelnosti/ministarstvo-kulture-i-informisanja:-nuns-i-ndnv-za-gasenje--vlada-za-opstanak-medija

Individually, the largest sum of money was awarded in Pirot, where three online media outlets received a total of over RSD 4,800,000 or RSD 1,600,000 per online media on average.



Average sum of money awarded to online media per city

Among the online media that received money from public funds, most were registered in 2015, when project funding provisions came to effect.

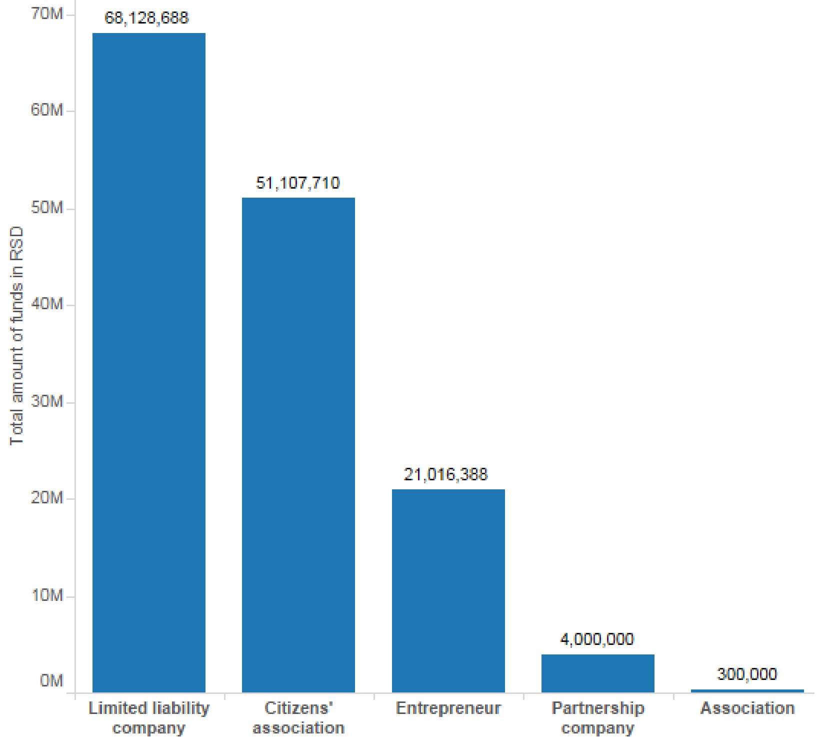


Total funds awarded to online media per registration year

Out of 520 online media organizations reviewed at the end of January 2017, 133 received funds based on project financing, i.e. 26% of all. Compared to the number of online media registered in a given year, budget allocations are relatively even and rarely exceed one third:

- 2009 - 36.8%
- 2010 - 20.9%

- 2011 - 25%
- 2012 - 28.1%
- 2013 - 30.5%
- 2014 - 45.7%
- 2015 - 33.6%
- 2016 - 22.6%



Number of online media awarded with funds per legal founder

Since all registered media are legally required to report funds received from public sources, whether at the national, regional or local level, data of co-financing is publicly available at the Media Register. According to available information, a total of RSD 68,579,196 was allocated to 81 online media in 2015, and a year later 106 online media received a total of RSD 75,739,280. As the most notable source of public financing, the Ministry of Culture and Information is also an important decision maker when it comes to setting the national course for implementation of public policies. In the first year of allocation of funds to the media in line with the newly adopted model, the Ministry issued six public calls for project proposals, of which the call for co-financing media production projects dealing with general public information was divided into two semi-annual cycles, and had the largest budget of RSD 164 million.

A total of 228 projects of printed and electronic media and productions were selected. In the first cycle, out of the 161 selected projects, 25 were proposed by online and citizen media that distribute content on the Internet. They received funds ranging from RSD 72,000 to RSD 2 million. [60] Out of those 25, 12 projects were awarded sums up to half a million RSD individually; sums of around RSD 700-800,000 were awarded to five projects, and another five received one million RSD each. One project was awarded with about RSD 1.5 million, and two received RSD 1.9 million.

The second cycle in 2015 had a considerably smaller budget: there were 67 selected projects in total, of which 13 were proposed by online and citizen media.[61] On this occasion, the funds allocated for online publications were even, ranging from RSD 450,000 to 600,000.

Overall, the Ministry allocated some RSD 25 million for general public information on the Internet in 2015, while in the following year this amount was close to 28 million.

After the 2016 call for projects was closed, there were 176 projects awarded with RSD 151,410,000.[62] Out of the total of 36 online and civil society online media projects, 20 were awarded with half a million dinars each. The next eight projects received less than a million, four were awarded one million, two received 1.5 and 1.7 million respectively. One project was co-funded with a sum of RSD 2.5 million.

If an evaluation of the selected projects is carried out, the Ministry of Culture does not make the process nor the results publicly available.

The media community does not analyze the results of selected projects and their effects either. A survey carried by the Serbian branch of the BIRN regional network reviewed the first year of the new state funding model, analyzing 30 projects that mostly represent examples of a well-executed plan.[63]

Among the analyzed projects, there were six that were produced by online media: Jug press, Juzne vesti, Vojvodina Research and Analysis Center (VOICE), the portal of the Association of Journalists of Serbia (UNS), "Whistle" – the research portal of the Eutopia Association, and Agropress – the website of the Association of Agricultural Journalists.

With the exception of the UNS project, aimed at the media community itself, and the Agropress production that was rated as unsatisfactory, other online media projects justified their role in informing the general public on important issues. They had been investigating state owned companies, use of public funds, political parties' influence on employment in public administration, and corruption at the local level.

[60] The distribution of funds, 11/05/2015 [in Serbian] http://www.kultura.gov.rs/docs/konkursi/19919583532220160079/RESENJE 20OPSTI 20KONKURS.pdf

[61] The distribution of funds, 20/11/2015 [in Serbian] http://www.kultura.gov.rs/docs/konkursi/15328113138329153612/RESENJE,kona C4 8Dno.pdf

[62] The distribution of funds, 22/07/2016 [in Serbian] http://www.kultura.gov.rs/docs/konkursi/82925044729285405888/Resenje, 20proizvodnja 20medijskih 20sadrzaja.pdf

[63] Project financing of the media: First year results of applying a new budget model, BIRN Serbia 2016. [in Serbian] http://birnsrbija.rs/wp-content/uploads/2016/12/Projektno-finansiranje-medija-Ministarstvo-kulture-i-informisanja.pdf

BIRN Serbia conducted a similar analysis of budget allocations in Vojvodina, i.e. the call for media proposals by the Vojvodina's Secretariat for Culture, Public Information and Relations with Religious Communities, where a total of RSD 53 million was allocated for private companies and civil society organizations in 2015. However, only about 34.3 million were awarded in the end, due to the committee's decision that there were not enough quality projects proposed. In 2016 the allocated budget was reduced six times, with only RSD 8.5 million awarded to 48 projects, as opposed to 2015, when over 100 projects received financial support. Again, there is no publicly available information on produced content and related costs, or analysis of the extent to which general public information was improved through project financing.[64]

In 2015, the online media owned by private companies and civil society organizations that proposed projects to the Provincial Secretariat open call[65] received a total of about RSD 2,900,000. In 2016[66] online media projects were co-financed with just a little over RSD 1,200,000, or around RSD 135,000 each on the average. Concerning co-financing online information projects in minority languages, only Hungarian "Vajdasag ma" portal received funds from the budget of Vojvodina in 2016, amounting to RSD 168,000. By comparison, the same portal received more than double the amount (RSD 366,000) a year earlier.

Press associations and related groups point to the fact that public funds are increasingly used to subsidize projects of media outlets that frequently breach the Serbian Journalists' Code of Ethics, thus forcing citizens to finance publishing of false stories and speculations, violations of presumption of innocence and of right to privacy. The Press Council proposed amendments to the Ministry's rules of open calls,[67] asking that decisions of its Press Complaints Committee are taken into account when selecting projects that would receive money from public sources. At the beginning of 2017 the State Secretary for Information at the Ministry stated that the proposal of the Press Council was acceptable, and that the Ministry was working on amendments to the Law on Public Information and the Law on Electronic Media.[68]

[64] Results of the first year of the implementation of the new budget model - Provincial Secretariat for Culture and Public Information of Vojvodina, BIRN Serbia [in Serbian] http://birnsrbija.rs/wp-content/uploads/2016/08/Projektno-finansiranje-medija-AP-Vojovodina.pdf

[65] Provincial Secretariat for Culture and Public Information of Vojvodina, results of the 2015 open call [in Serbian] http://www.kultura.vojvodina.gov.rs/Konkursi/rez _ inform _ 15/rezul _ inform _ 15.htm

660Provincial Secretariat for Culture and Public Information of Vojvodina, results of the 2016 open call [in Serbian] http://www.kultura.vojvodina.gov.rs/Konkursi/rez _ inform _ 16/rezultat _ inform _ 16.htm

[67] Rulebook on co-financing projects of public interest in the area of general public communication [in Serbian] http://www.kultura.gov.rs/docs/dokumenti/propisi-iz-oblasti-medija/pravilnik-o-sufinansiranju-projekata-za-ostvarivanje-javnog-interesa--u-oblasti-javnog-informisanja--.docx

[68] Citizens will again fund the media that publish false stories, Insajder [in Serbian] https://insajder.net/sr/sajt/tema/2927/Gra C4 91ani- C4 87e-opet-finansirati-i-medije-koji-iznose-neistine.htm

RECOMMENDATIONS

To encourage public calls for co-financing online media projects, especially those concerning local communities, informative, scientific and educational projects, as well as those published in minority languages. Online media are more economical and make a significant contribution to pluralism in general public information. To include decisions of Press Complaints Committee to the set of criteria when selecting projects to be funded by the state.

GUIDE:

LEGAL STATUS OF ONLINE MEDIA IN SERBIA

"Legal Status of Online Media in Serbia" is a guide which presents new solutions brought by the Law on Public Information and Media that are relevant to online and citizen media. Digital platforms such as blogs, forums, social media, and independent news sites are not considered media by the Law unless they choose to register. The guide gives an overview of rights and obligations that online media assume if they register, explaining differences in liability for the content published in a registered media outlet from the general legal regimen, as well as the registration process itself.

Media's legal status provides additional rights, such as protecting the identity of a source of information, higher standards of protection of personal integrity of journalists, or access to state funding. Assuming special rights entails certain obligations, like due diligence, that is verification of sources, truthfulness and completeness of information prior to publishing, keeping media records, transparent ownership, while the media publisher, editor, and journalist have extensive responsibility for content in line with the Law on Public Information and Media.

(The Guide published in March 2016)

2.4. ONLINE MEDIA AND SELF-REGULATION

Online sources, such as portals, blogs, and social media enable a more diverse range of available information, nonlinear tracking of related content, and a more immediate engagement of audience in creating and distributing the news. However, the speed with which information is disseminated on the Internet, as well as the absence of selection of participants in public discourse, have caused, among other things, an uncontrolled proliferation of unethical and unprofessional journalism, misconduct, threats to privacy, violation of the presumption of innocence. If citizen journalists and free platforms want to adhere to true, timely and complete information they publish, they need to honor the provisions of the Code of Ethics, regardless of whether they are professional journalists or not.

The Press Council was established in Serbia as late as in 2009, as an independent, self-regulatory body observing the Serbian journalists' Code of Ethics. The Council had full authority over print media and their Internet editions, but recently this body established an instrument of limited authority over the media organizations that have not accepted its full authority. This has enabled reviewing complaints against any print media, news agency, or news portal for breaching the Code of Ethics.[69]

The Internet has posed new ethical challenges for the media and professional journalists, making it difficult to apply some of the Code's provisions to content published on online platforms. Therefore, in 2016, the Council prepared Guidelines for online application of the Code of Ethics, the first official document of this kind in the region, interpreting the ethical principles of the profession in the new technical environment.[70] In order to deal with the new challenges, the Guidelines provide clear instructions to journalists, editors, and media managers, readers and advertisers, and also to the Press Council's Complaints Commission.

"This document is primarily intended for online journalists and media outlets, but it is also applicable to other forms of expression on the Internet, where editorially shaped media content is distributed through various platforms. The aim is to clarify the many doubts concerning the standards of journalistic due diligence, the approach to sources of information, the ways in which media content is distributed, respect for privacy, respect for authorship, and other important issues regulated by the Code," reads the Preamble of online guidelines of the Press Council.

Each of the 10 chapters of the Serbian journalists' Code of Ethics has been interpreted for the online environment and extended to specific media-related factors, while some areas, such as user generated content, gathering information from social media, and copyright, are described in more detail. Guidelines are a significant tool in the process of raising the level of digital literacy of journalists and the audience.

Among else, the principle of truthfulness applied to the media that store and share information on the internet implies the ban on modification of digital traces, subsequent alteration of content without indication of the character of changes, antedating of the published content, and so on. Due diligence online also extends to social media and other platforms of informal exchange of information, while official social media accounts are also considered to be editorially shaped content. The integrity of authors and copyrights is in full effect in an online environment, particularly in regard to digital processing tools, aggregators, and the like.

RECOMMENDATIONS

To foster the development of self-regulation, compliance with the Serbian journalists' Code of Ethics, and the authority of the Press Complaints Committee. To provide support for further development of ethical rules of general communication online. To encourage online media, organizations with online presence, citizen journalists and other Internet actors involved in reporting on issues of public concern, that do not want to formally register as media, to nevertheless comply with the Code of Ethics and the decisions of the Press Complaints Committee. To promote self-regulatory mechanisms within the Internet community. To strengthen the principle of post-moderation of third party content. To promote mechanisms for swift and transparent flagging of harmful and illicit content.

[69] In October 2013 the SHARE Foundation filed a complaint on behalf of Simon Wilson against the website "Teleprompter", which was not formally registered nor a member of the relevant associations. The Press Council confirmed its the jurisdiction and issued a public warning to the website: [in Serbian] http://www.shareconference.net/sh/defense/savet-za-stampu-portal-teleprompter-prekrsio-kodeks-novinara-srbije

[70] Guidelines for the online application of the Code of Ethics [in Serbian] http://www.savetzastampu.rs/latinica/smernice-za-primenu-kodeksa-novinara-srbije-u-onlajn-okruzenju

GUIDE:

ONLINE COMMENTS: GOOD PRACTICE AND MODELS

Digital media, besides online press editions, radio and television, include a number of other platforms, such as news portals, blogs, search engines, social media, online stores, video sharing websites, news aggregators, and alike. The backbone of these services is user-generated content that contributes to interactions (likes, retweets, favorites) and to the revenue of the platform. Various interaction features attract more users, prompting advertisers to place their ads.

Online comments enable news sites and other platforms to try and match social media traffic. Practices that reduce the visibility of comments and disable their immediate posting, such as pre-moderation, considerably slow down user interaction, limit discussions and free flow of information, which also adversely affects the attractiveness of media websites for advertisers. On the other hand, a comment section without moderation control exposes media to legal risks.

(The Guide published in October 2015)

2.5. AGREEMENT ON MEDIA, POLICE AND PROSECUTION COOPERATION

RECOMMENDATIONS

To operationalize the collaboration of the police and prosecutorial offices with the online media that are commonly the target of cyber attacks, in order to exercise more efficiency in dealing with threats to cyber security. To overcome the legal insecurity stemming from inconsistent decisions on who is entitled to special journalistic privileges.

As an important step towards improving the safety of journalists, an agreement on cooperation and relevant measures was signed between representatives of the Ministry Interior Affairs, the Public Prosecutor's Office, and seven press and media associations.[71] Technical attacks against online media and threats to journalists on social media have threatened the freedom of expression for some time. An additional problem the SHARE Foundation points out is the selective legal protection by authorities.[72]The cases of swift and efficient police and prosecutorial reactions related to protection of officials are increasingly disproportionate when compared to cases in which journalists, especially those engaged in investigative and dissenting work, have long waited for the outcome of procedures concerning threats and pressure against them. The formal agreement on cooperation of press associations and relevant state agencies represents a significant step in providing legal certainty and trust in investigations into attacks against journalists and media organizations.

The agreement outlines a system of measures to "provide a more effective criminal justice protection for journalists". Ten activities were agreed upon, among which the most important is the establishment of a working group for the implementation of the agreement whose members will be authorized representatives of the signatories; the appointment of contact persons; the keeping of records of criminal offenses against journalists; the creation of a register of criminal offenses against journalists, media and news portals; training journalists and media owners on the basics of cyber security. The agreement also provides training of staff at the Ministry and the Prosecutor's Office.

The promotion of protection measures through immediate cooperation of the media community and relevant state agencies contributes to the prevention of violations of rights. A consistent enforcement of law in cases of threats, pressure, physical attacks and high-tech crime, is an indispensable factor of the rule of law. The Ministry of Interior Affairs and the Public Prosecutor's Office have agreed to implement the obligation to act urgently in criminal offenses against journalists in their internal rulebooks, within three months of signing the agreement. An emergency response to cases of threats in the digital environment and cyber-attacks against journalists and news portals, should become a priority of the police and prosecution services, especially since previous cases of technical attacks on dissenting and investigative websites (such as Pescanik or CINS) have not yet been resolved after almost three years. Investigation of numerous cases of threats aimed at journalists on social media and comment sections have also remained without any legal resolve.

[71] Agreement on cooperation and relevant measures for improving safety of journalists [in Serbian] http://www.aom.rs/wp-content/uploads/2016/12/Sparazum-o-saradnji.pdf

[72] Selective protection, SHARE Foundation, 2015 [in Serbian] http://www.shareconference.net/sh/blog/selektivna-zastita

GUIDE:

CONFIDENTIALITY OF SOURCES

Relying on anonymous sources is crucial to reporting on issues of public interest that citizens would otherwise be unaware of. Some of the most significant stories in the history of journalism (such as the "Watergate" affair in the USA) were made thanks to information gained from the sources whose identity was hidden from the public. On the other hand, inventing and abusing anonymous sources are gross violations of professional and ethical standards.

In various forms of digital communication, public information is no longer reserved solely for journalists of traditional media organizations numerous internet platforms, blogs, forums, social media and independent online outlets, enable citizens to participate in reporting on social issues and problems. Since it can be said that social media users play a similar role as journalists, do they need protection similar to the protection of sources? Answers to this and similar concerns can be found in relevant rules, recommendations, international experiences, and jurisprudence.

(The Guide published in October 2015)

2.6. LEGAL PROCEEDINGS AND COURT DECISIONS

RECOMMENDATIONS

To enhance capacities of the judiciary for applying the regulatory framework to online media. Through education of the police, the prosecution, the judiciary, and lawyers, to establish the practice of continual training on the features of the digital environment, risks, and protection of the freedom of speech in the context of general communication on the Internet. To ensure equal efficiency of the judiciary in processing violations and threats to citizen rights on the Internet, regardless of who the target is, in order to avoid the legal uncertainty of selective protection.

The SHARE Foundation monitors the legal development of particular cases, their legal classification and court decisions. The incidents occurring in cyberspace rarely enter court proceedings, their legal treatment does not always reflect a full understanding of violations in an online environment, while the proceedings themselves, whether litigious or criminal, last for quite a long time, even years.

1. ZORAN PERISIC V. JUZNE VESTI

Former mayor of Nis Zoran Perisic sued the Juzne Vesti news portal for slander on account of publishing the text "Spasic: Authorities Ateal Workers' EI Money" of September 2014. In the first instance the High Court in Belgrade ruled in favor of Perisic, but Juzne Vesti filed an appeal against the verdict.[74]

2. PUBLIC PROSECUTOR V. RADOMIR POCUCA

Former spokesperson of Serbia's counter-terrorist police unit Radomir Pocuca was released from accusations of having committed a criminal offense of endangering security. The verdict was passed by the High Court in Belgrade, with the written decision to be subsequently issued. Criminal proceedings against Pocuca were initiated because in 2014 he posted a text on his Facebook page which allegedly incited violence against members of the NGO Women in Black.[75]

3. PUBLIC PROSECUTOR V. JELENA POPOVIC IVANOVIC

A teacher at the High School of Technical Sciences in Novi Sad, Jelena Popovic Ivanovic was sentenced to three months' imprisonment, with a one-year probationary period, due to her Facebook post made in 2011 promoting hate and intolerance against LGBT population. The Belgrade Court of Appeal upheld the first instance verdict of the High Court in Belgrade of May 2016 for the criminal offense of racial and other discrimination.[76] The verdict is not yet available.

4. OFFICIALS V. CITIZENS

According to "Pistaljka", the investigative news portal, the police from the town of Bogatic interviewed at least two citizens in late 2016 to determine who insulted three local officials, including municipality president Nenad Beserovac, by posting on the Facebook page "Macva of Healthy Reason". After the complaint filed by the officials, the public prosecutor's office in Sabac stated that it found no elements of criminal offense for an ex officio prosecution, but it also indicated that the police in Bogatic should take all measures and actions in order to identify persons who offended the officials so that the officials could sue.[77]

ENDANGERING SAFETY VIA THE INTERNET

Verdicts issued in 2016 that are of significance for understanding human rights in an online environment and provide an insight into the stance of courts when applying laws to content sharing platforms and social media.

1. BORIS MALAGURSKI V. FORUM MEMBERS

On 28/08/2012 a debate was launched on a local message board called "Parapsihopatologija" in which the defendants made insulting comments. The injured parties filed criminal charges in September 2012 against 12 forum members on account of organized threats to life and personal and professional safety under Article 138, paragraph 3 of the Criminal Code. The identity of the three alleged perpetrators against whom criminal proceedings were initiated, was discovered by internet providers Orion Telekom and SBB.

[74] Ruling in favor of Perisic v. Juzne Vesti, November 2016 [in Serbian] http://niskevesti.rs/presuda-u-korist-perisica-protiv-juznih-vesti/

[75] Pocuca freed for threats to Women in Black, his passport returned, December 2016 [in Serbian] http://www.kurir.rs/crna-hronika/izrecena-presuda-pocuca-osloboden-za-pretnje-zenama-u-crnom-i-vracen-pasos-clanak-2588901

[76] Professor at Technical High on probation for spreading hate against LGBT, September 2016 [in Serbian] http://www.021.rs/story/Novi-Sad/Vesti/144105/Profesorki-Srednje-masinske-uslovna-kazna-za-sirenje-mrznje-protiv-LGBT-populacije.html

THE ENSUING PROCESS CONSISTED OF SEVERAL STAGES:

1. First instance: On 11/03/2014 the High Court in Belgrade convicted the three indictees, sentencing them to one year imprisonment, provided that the defendants do not make a new criminal offense within a period of three years. There were procedural mistakes, so the decision was revoked, and the High Court again made a convicting decision on 24/03/2015, sentencing the defendants with the same penalties.
2. The second instance after the defendants' appeal: On 09/09/2015 the Court of Appeal in Belgrade partially accepted the arguments of the defense counsels, overturning the initial verdict so that two defendants were now sentenced to 6 months in prison, with two years' probation, and one of the defendants was sentenced to 4 months in prison, with two years' probation. The appeal was therefore successful in reducing the sentences.
3. Extraordinary Legal Remedy: The defendants filed a claim for protection of legality, which was an extraordinary legal remedy, and on 20/01/2016 the Supreme Court of Cassation decided on acquittal.

ANALYSIS OF THE VERDICT OF THE SUPREME COURT OF CASSATION (1203/2015 OF 20/01/2016)

The Supreme Court of Cassation stated that upon a request for protection of legality it was established that a law that could not be enforced was applied, which meant that the actions that had been taken could not be considered a criminal offense of endangering safety.

The Court ruled that the initial verdict was missing an essential element of the criminal offense of endangering safety, which is a threat to attack the life and body of the injured parties. For an act to be an element of a criminal offense, the threat must be serious and must involve an attack against the life or body of the injured person. When it comes to verbal threats announcing the attack, which was the case on this occasion, those must be clear and unambiguous, so that it can be concluded from the threat that the perpetrator would indeed attack the injured person, regardless of whether they actually intend to do so.

After analyzing each individual post allegedly constituting the matter of this case, the Court concluded that these were statements of what the defendants thought should be done to the injured party, what kind of feeling the defendants had in relation to the injured party, and what the defendants would like to be done to the injured party, but they did not present clear and unambiguous threats that the accused parties were in fact going to attack the life and body of the injured parties.

The Court found that the verdict pronounced was based on the wishes of the defendants to have any harm done to the injured party, and not on statements that the defendants would be doing that harm. Therefore, the defendants were released.

[77] The police investigates who insulted the officials, December 2016 [in Serbian] https://pistaljka.rs/home/read/578

2. JUZNE VESTI V. READERS

A criminal complaint made by the online media outlet Juzne Vesti against visitors leaving threatening comments, was also resolved in court. The threats read: "Juzne Vesti are the biggest media shit in Nis, they should be burned down so they do not exist no more, lying, frustrated degenerates that are working there". [78]

The final verdict of the High Court in Nis confirmed the first instance ruling of the Primary Court in Nis in favor of the defendant. In this case, the Court also came to the conclusion that no actual threat could be established because the defendant "did not express his personal intention at any moment to take any action that could harm the safety of the injured party. If the defendant were expressing his personal intentions to take action against the injured party, regardless of whether these intentions were real, than it could be said that there was a criminal offense of endangering safety."

Reviewing the decisions of relevant courts in Serbia it could be concluded that the processes initiated on account of alleged threats to safety, mostly lack the essential element of this offense, namely serious, clear and unambiguous threats, as well as personal intent to attack the life and body of the individual against which the threat is directed. In each individual case the whole context in which the information has been published must be taken into account, with the analysis of all the words expressed.

3. INSULTS AGAINST SOCIAL MEDIA - JUDICIAL PRACTICE IN CONFLICT

The Supreme Court of Cassation also dealt with the case of a defendant I.P. who filed a request for the protection of legality against the rulings issued by the Primary Court in Novi Sad (K 266/15 of 21/12/2015) and by the High Court in Novi Sad (Kz1 110/16 of 24/06/2016).[79] In this case, a person was convicted of an extended criminal offense pursuant to Article 170 paragraph 2 of the Criminal Code, and sentenced to a fine of RSD 250,000.00, for having offended the plaintiff by posting multiple texts on their Facebook page.

After reconsidering the case, the Court came to the conclusion that the appeal was unfounded, confirming the guilty verdict. The defendant claimed in their appeal that the Facebook page cannot be considered a means of general public communication, but the claim was rejected. "[...] the Supreme Court of Cassation finds that a Facebook page, due to its availability to users on the Internet, can be considered a means similar to print, radio or television, and consequently this similar means of a Facebook page can be used for expressing an insulting statement and thereby committing a criminal offense of insult."

The decision of the Supreme Court of Cassation that Facebook is "similar to press, radio or television" differs from the conclusion of the High Court in Belgrade made in a final ruling of a case in which an insult was addressed

[78] The Court: "Journalists should be burned" is not a threat but a freedom of speech, July 2016 [in Serbian] https://www.juznevesti.com/Drushtvo/Sud-Treba-zapaliti-novinare-nije-pretnja-vec-sloboda-govora.sr.html

[79] Supreme Court of Cassation, Kzz 1058/2016 [in Serbian] http://www.vk.sud.rs/sr-lat/kzz-10582016

on 25/08/2015.[80] Namely, in the first instance proceedings, the Primary Court in Belgrade deliberated on the accusation of the criminal offense under Art. 170 paragraph 2, constituting a qualified form of crime made via press, radio, television or similar media or a public gathering. However, the High Court revised this judgment, referring to the provision of Article 11 of the Public Information Law, which was in force at the time of the alleged criminal offense. This provision stipulates that public media are "newspapers, radio programs, television programs, news agency services, the Internet and other electronic editions of the afore mentioned public media [...] intended for public distribution to an indefinite number of users". The High Court ruled that social media "represent a group of individual Internet users connected for interpersonal communication and exchange of information, opinions and ideas among members", and that therefore social media could not be considered similar to press, radio or television "that represent general public information media and are intended for public distribution to an indefinite number of users".

This ruling of the High Court was also in line with the new Law on Public Information and Media, which in Article 30, paragraph 2, unambiguously defines what is not considered to be media, i.e. the definition explicitly excludes forums and social media.[81] Considering the entire legal framework, the definitions that were in force in both the old and the new law, the decision of the Supreme Court of Cassation is a precedent that directly threatens the freedom of opinion and expression.

Apart from the fact that Article 170, paragraph 2 of the Criminal Code, cannot be applied to the social media, particularly in the light of the new, clear provisions of the Public Information and Media Law, attention should be drawn to the Criminal Code provisions that still define defamation as a criminal act, despite international trends of decriminalization of defamation and insults. The Republic of Serbia decriminalized defamation in 2013, but for reasons yet unclear the insult remained in the criminal system. A criminal offense of insult constitutes a statement or other act which, by objective assessment, degrades a particular person. This broad definition, however, enables applying this provision practically to any statement made in social media. If the decision of the Supreme Court of Cassation establishes a new practice, that is to say that Twitter or Facebook should be treated as press or television, any harsh online comment could also be treated in a qualified form of an act made through means of general public communication.

There is still not enough knowledge of all possibilities and risks of the Internet as a new media environment, while it seems that national courts lack the understanding of online communication, its technical characteristics, and ways to apply the law in the online sphere. Advanced skills and new standards in relevant institutions, as well as raising the sense of responsibility among internet users themselves, should ensure positive development of court practice.

[80] Ruling Kž1 br. 465/15

[81] Law on Public Information and Media, Official Gazette of RS, no. 83/2014, 58/2015 and 12/2016 [in Serbian] http://www.paragraf.rs/propisi/zakon_o_javnom_informisanju_i_medijima.html

3. INFORMATION PRIVACY

In response to a request for free access to information of public importance, in April 2014 the SHARE Foundation obtained 2000 pages of documents and reports from the Commissioner for Information of Public Importance and Personal Data Protection, containing the Commissioner's Report on the check of enforcement and compliance with the Law on Personal Data Protection by mobile and fixed telephone operators in Serbia. These documents served as the basis for analyzing metadata retention and electronic surveillance architecture.

Technical and legal analyses of these documents, presented through a series of infographics, illustrate different ways in which four operators of mobile and fixed telephony in Serbia enable state bodies to directly access users' metadata. It is important to highlight that any device, whether it is a smartphone or an older generation phone, generates metadata. The only significant difference between these devices is that older phones cannot be used for internet access. Therefore, this research was carried out with a focus on smartphones.

In order to connect to the network, the device uses two identification numbers: the IMEI device number (International Mobile Station Equipment Identity) and the IMSI SIM card number (International Mobile Subscriber Identity). Both of these numbers are unique and predefined for every device and SIM card. Base stations (BS) make up the mobile operator's infrastructure and they are geographically positioned in the area covered by the mobile operator.

When initiating a call, the caller's device contacts the nearest base station which then forwards the call to the Mobile Switching Centre. The MSI then notifies the base station nearest to the device of the call recipient, and the connection is established. When the connection is live, i.e. when the recipient answers the call, metadata are generated in the MSI, which stores the metadata into the operator's data centre. The content of the call is not archived, but it also passes through the MSI.

TYPES OF METADATA ARCHIVED

Different switching centers collect different types of metadata, but there is a general class of metadata archived by all operators, such as the caller's phone number, the recipient's phone number, IMEI, base station details, date and time of the call, data amount (for Internet), type of service, identity of both sides involved in communication, the list of all SIM cards used in a particular device, and vice versa – the list of all devices in which the specific SIM card was used.

METADATA STORAGE

Operators in Serbia are legally obliged to store each user's metadata for 12 months. It is not strictly defined whether they are obliged to own servers for this purpose, or they can use servers from another company.

ACCESS TO METADATA

Mobile operators in Serbia have formed departments that deal with data retention procedures, with specially trained staff. Access right is reserved for specific state institutions: judicial bodies, police, and civilian and military intelligence services.

The largest operators in Serbia have implemented two mechanisms for accessing retained data. The first one is activated upon a request that the operator receives, reviews and responds to: in their request, state authorities indicate which data exactly they want to access, after which the operator processes the request and submits a report. In order to prove authorization, the request needs legal grounds, which is a relevant court order.

The other mechanism used to access retained data is controversial from the legal point of view, since it uses autonomous application software enabling direct access to data. This software was implemented by some operators to make access to retained data easier for state authorities, bypassing the procedure and practically enabling access without a court order, which is a violation of the Constitution.

In recent years, many bylaws have been passed defining the rights and obligations of operators and state authorities regarding the interception of electronic communications. Among else, these rules provide that it is the operator's duty to buy the equipment needed for intercepting communications (hardware and/or software) and deliver it to the monitoring center run by the Security Information Agency (BIA).

PHYSICAL REAL-TIME TRACKING

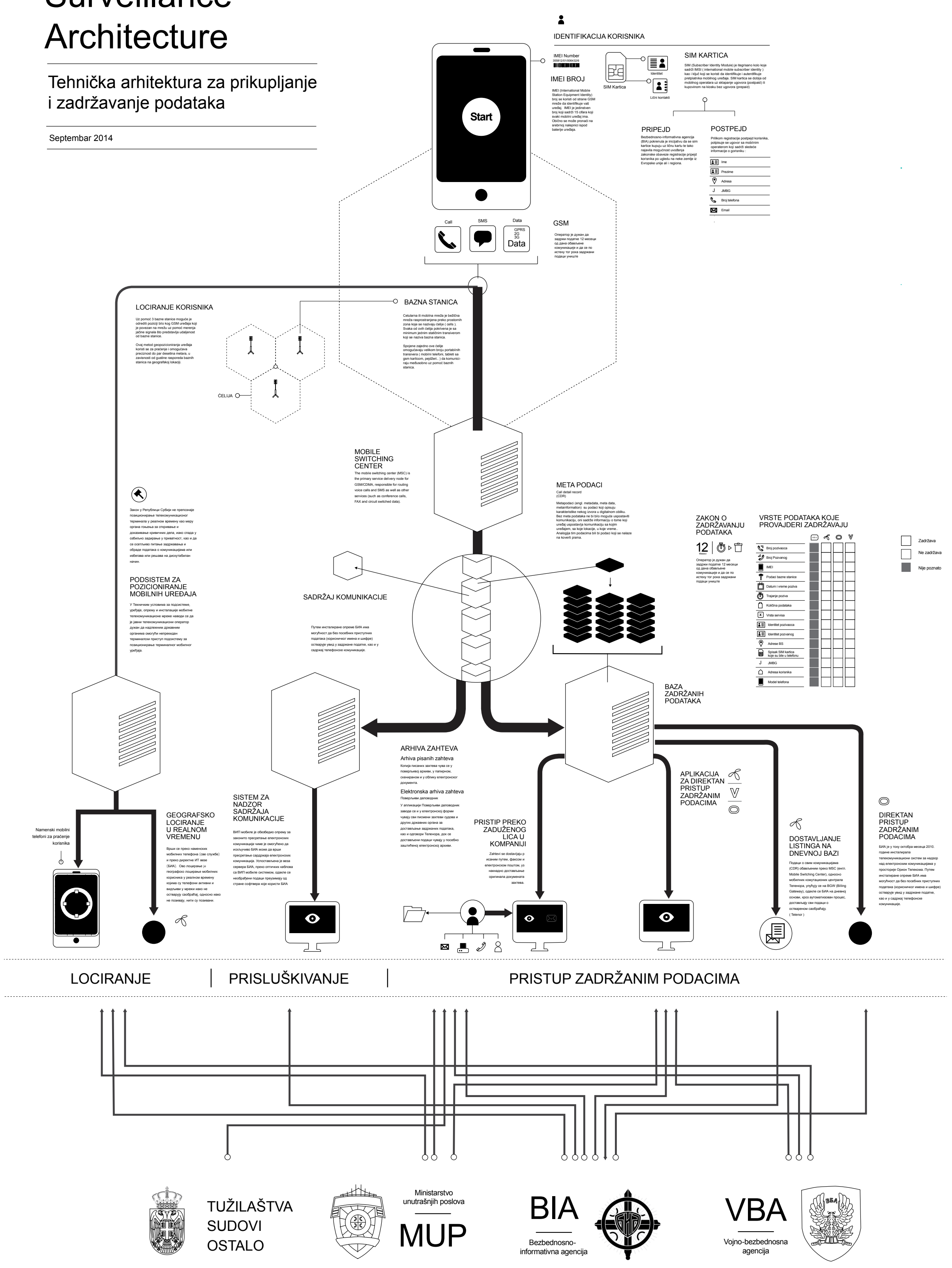
Base stations represent "cells" of an operator's infrastructure which form a cellular network through interconnection. A cell is in fact a geographic area covered by one base station. At any given moment, a device used for communication (cellphone, tablet) is connected to three base stations in order to secure continuity of the signal - that means that three base stations constantly exchange incoming and outgoing signals with the device. Base stations are set up in such a way that they record the distance of the device, i.e. determine its location based on several parameters. Some of those parameters are the angle of arrival (AOA), the time difference of arrival (TDOA) and the time of arrival (TOA). This means that anyone with access to a base station can determine at any moment the physical location of any device connected to the network with a high level of precision.

In line with relevant bylaws, SIA has access to special terminals of device tracking equipment. Also, there are mobile devices made upon special request, configured to enable real-time geo-tracking. These mobile devices are issued by operators to state authorities when requested. This means that anyone who has access to the terminal of this equipment can determine the exact location of any device connected to the mobile network in Serbia.

Surveillance Architecture

Tehnička arhitektura za prikupljanje i zadržavanje podataka

Septembar 2014

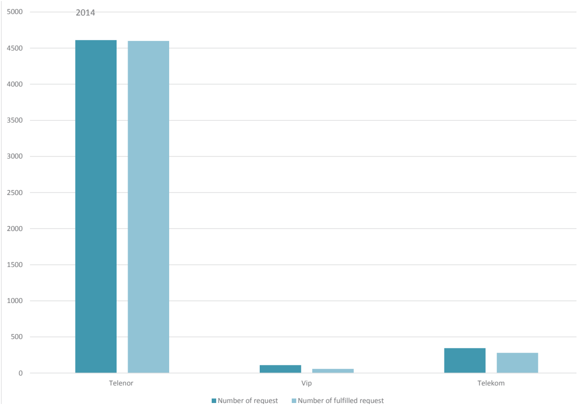

IDENTIFIKACIJA KORISNIKA
IMEI BROJ
SIM Kartica
SIM KARTICA
PRIPEJD
POSTPEJD
Start
Call
SMS
Data
GSM
LOCIRANJE KORISNIKA
BAZNA STANICA
ĆELIJA
MOBILE SWITCHING CENTER
META PODACI
ZAKON O ZADRŽAVANJU PODATAKA
VRSTE PODATAKA KOJE PROVAJDERI ZADRŽAVAJU
12
Zadržava
Ne zadržava
Nije poznato
PODSISTEM ZA POZICIONIRANJE MOBILNIH UREĐAJA
SADRŽAJ KOMUNIKACIJE
BAZA ZADRŽANIH PODATAKA
ARHIVA ZAHTEVA
Arhiva pisanih zahteva
Elektronska arhiva zahteva
APLIKACIJA ZA DIREKTAN PRISTUP ZADRŽANIM PODACIMA
DIREKTAN PRISTUP ZADRŽANIM PODACIMA
DOSTAVLJANJE LISTINGA NA DNEVNOJ BAZI
PRISTIP PREKO ZADUŽENOG LICA U KOMPANIJI
SISTEM ZA NADZOR SADRŽAJA KOMUNIKACIJE
GEOGRAFSKO LOCIRANJE U REALNOM VREMENU
Namenski mobilni telefoni za praćenje korisnika
LOCIRANJE
PRISLUŠKIVANJE
PRISTUP ZADRŽANIM PODACIMA
TUŽILAŠTVA
SUDOVI
OSTALO
Ministarstvo unutrašnjih poslova
MUP
BIA
Bezbednosno-informativna agencija
VBA
Vojno-bezbednosna agencija

3.1. ELECTRONIC SURVEILLANCE: STATISTICS

The most common way in which a state surveils citizens in the era of new technologies, is electronic surveillance of retained information. Serbia is no exception in this respect. In April 2014 the European Court of Justice (ECJ) declared the EU Data Retention Directive invalid,[82] followed by several member states revoking relevant national laws as unconstitutional.[83] Serbia has not yet taken the question of rules imposed on telecommunication operators into consideration, and companies providing services of fixed and mobile telephony and the Internet continue to retain their users' data, making them available to investigative and other agencies.

According to the reports the operators submitted to the state Commissioner for Public Information and Personal Data Protection in 2014 and 2015, there was a rising trend in requests for access to retained data but in autonomous access as well, without using protective measures prescribed by the Law on Electronic Communications.

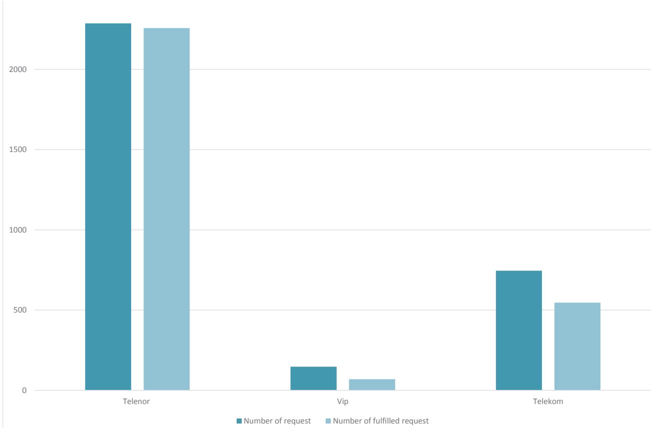
The second largest telecommunications operator in Serbia, Telenor, registered far more access requests filed in 2014 and 2015 by state agencies (police, courts, civil and military intelligence agencies) than the state owned Telekom, the largest national operator by the number of users. In 2014 Telenor registered 4611 requests, out of which 4599 were accepted, while out of 2287 requests received in the following year, Telenor accepted 2257. At the same time, according to Telekom's annual reports, this company received only 344 requests for access to retained data in the second half of 2014 , out of which it accepted 280. In the following year, Telekom received a total of 745 requests and accepted 546 of them. The third operator, Vip, reported only 109 requests in 2014 (58 accepted) and 147 in 2015 (69 accepted).



Number of received and accepted requests for retained data access in 2014

[82] ECJ Invalidates Data Retention Directive, June 2014 https://www.loc.gov/law/help/eu-data-retention-directive/eu.php

[83] Data Retention Laws By Country, February 2016 https://www.goldenfrog.com/blog/global-data-retention-lawsl



Number of received and accepted requests for retained data access in 2015

Among large operators who submitted reports to the Commissioner, only Telenor acknowledges registering direct access of government agencies to the company's ICT system for the purpose of collecting retained data. The frequency of autonomous access is much higher than the number of filed requests, suggesting a possibility of random browsing through all the retained data in search of the data needed.

In 2014 Telenor's ICT system registered 201,879 events of autonomous access to retained data, namely: Police (MUP) 199,818, Civil Intelligence Agency (BIA) 993, Military Intelligence Agency (VBA) 1068. In the following year, there were 300,845 events of autonomous access recorded.

3.2. TELECOMMUNICATION REFORM

The Ministry of Trade, Tourism and Telecommunications issued a call for participation in a public debate on the Draft Law on Electronic Communications, which took place from 14 November 2016 until 3 December 2016.[85] The draft of the new law[86] was supposed to replace rules adopted in 2010,[87] tackling two areas of importance for citizens' digital rights.

3.2.2. REGISTRATION OF PREPAID NUMBERS

Article 144 of the draft law on electronic communications prescribes mandatory "subscriber registration prior to the beginning of providing the service through the public mobile communication network" (Paragraph 1). It is not defined, however, which users have this obligation, leaving it open for a conclusion that registration will be compulsory for prepaid mobile phone users as well, which is not the case in the existing law. Based on experiences from countries where similar solutions have been adopted, as well as on analyses of the domestic legal framework, the SHARE Foundation took the position stating that mandatory registration of prepaid SIM cards in Serbia would be an intrusive measure, with no guarantees that it would indeed help combat crime and protect national security.

A particularly worrisome issue is that the mandatory registration was proposed without an adequate analysis of social and economic effects that would provide arguments as to why such a measure was necessary. In this regard, it is worth noting that the latest report by the GSM Association claims there is no empirical evidence of this practice directly affecting crime rate reduction. [88]

Within the public debate on the draft law, the SHARE Foundation sent its comments to the relevant Ministry, arguing that Article 144 of the presented Draft Law on Electronic Communications should be deleted from the final version. [89]

[85] Public debate on Draft Law on Electronic Communication [in Serbian] http://mtt.gov.rs/vesti/javna-rasprava-o-nacrtu-zakona-o-elektronskim-komunikacijama/?lang=lat

[86] Draft Law on Electronic Communication [in Serbian] http://mtt.gov.rs/download/Nacrt%20zakona%20o%20elektronskim%20komunikacijama.pdf?lang=lat

[87] Law on Electronic Communications ("Official Gazette of RS", No. 44/2010, 60/2013 – Decision CC and 62/2014) [in Serbian] http://www.paragraf.rs/propisi/zakon _ o _ elektronskim _ komunikacijama.html

[88] Mandatory registration of prepaid SIM cards, April 2016 http://www.gsma.com/publicpolicy/wp-content/uploads/2016/04/GSMA2016 _ Report _ MandatoryRegistrationOfPrepaidSIMCards.pdf

[89] SHARE Foundation's comments on Draft law on electronic communication, December 2016 [in Serbian] http://www.shareconference.net/sites/default/files/u742/komentari _ na _ nacrt _ zek _ share _ fondacija.pdf

3.3. PERSONAL DATA PROTECTION

3.3.1. WAITING ON A NEW PERSONAL DATA PROTECTION LAW

RECOMMENDATIONS

Adoption of a new law on personal data protection is among top priorities in this area. The process of drafting the text of the law has to include an appropriate public debate in order to find optimal solutions balancing the interests of citizens in protection of privacy and personal data on the one hand, with the interests of data economy and domestic and international companies on the other hand.

The existing Law on Personal Data Protection has been in force since 2008. Although it was the first law regulating this area in Serbia, with many contradictions and problems in its application from the very beginning, apart from minor amendments the Law is still in force in its original form. Until today, some of the key issues concerning data protection are left unregulated, such as video surveillance, biometrics, security audits, private security industry, and alike. It is needless to point out just how much the world has changed since the Law was written, and how complex the issue of personal data protection has become, as a consequence of the use of communication technologies and data economy development. However, the domestic legal framework is still unaware of these changes and complexities.

In April 2016, after a four-year long process, the European Parliament and the Council adopted the General Data Protection Regulation.[90] The harmonization of the domestic legal framework with this Regulation is certainly a top priority in this area, being Serbia's obligation in accession negotiation with the EU as defined in the Action Plan for Chapter 23. On the other hand, which is much more significant, the Regulation represents a new standard of protection of citizens' privacy and personal data, and ways in which the companies that process personal information operate.

[90] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680

The Commissioner for Public Information and Personal Data Protection developed a model of the new law by mid-2014, and presented it to the Government of Serbia. The Action Plan for Chapter 23 provides that future rules would be drafted in accordance with this Model. However, when a working group of the Ministry of Justice issued a call for a public debate on the draft of a new law in November 2015, it turned out that the proposed draft almost entirely ignored the Model. Significant points of divergence were explained in detail by the Commissioner,[91] while the SHARE Foundation offered comments on a series of questionable proposals as well, with the support of numerous civil society organizations.[92] The community's dissent was obviously taken into account, and after the public debate was closed the proposed draft was no longer mentioned by the officials.

Meanwhile, the Commissioner presented a new model for the future personal data protection law, "in line with current standards of relevant European documents, and primarily with the General Data Protection Regulation", calling for a public debate.[93] In April 2017 the SHARE Foundation held a consultative meeting, inviting relevant civil society organizations to present their comments on the Commissioner's new model, and to join a collective request to the Government of Serbia to draft and pass a new personal data protection law in the shortest possible time.

From this point in time, it seems that a suitable reform of the personal data protection legal framework was not possible before the new EU Regulation was adopted. It is therefore inevitable to conclude that the second half of 2016 should have been used for a comparative analysis of the GDPR and the domestic legal framework, with all the elements in place for a substantial reform.

Since time was missed, it is required that a new law is drafted as soon as possible, in accordance with the GDPR, with participation of expert and interested groups within a proper public debate.

[91] Poor draft of the law on personal data protection, November 2015 [in Serbian] http://www.poverenik.rs/yu/saopstenja-i-aktuelnosti/2228-slab-nacrt-zakona-o-zastiti-podataka-o-licnosti.html

[92] Comment on Draft law on personal data protection, SHARE Foundation, November 2015 [in Serbian] http://www.shareconference.net/sites/default/files/u742/share_fondacija_komentari_na_nacrt_zakona_o_zastiti_podataka_o_licnosti.pdf

[93] New Model law on personal data protection [in Serbian] http://www.poverenik.org.rs/sr/2017-03-06-09-09-59.html

Analysis of best practices and procedures for personal data protection applied in several selected institutions, based on the principles established during years of experience of the Commissioner's office and on the knowledge of SHARE Foundation in the field of protection of privacy in the digital environment.

The Guide is intended primarily for government authorities, but given that the personal data protection law applies to all relevant actors, studies and recommendations from SHARE's research would also benefit the data handlers from private sector. It represents significant contribution to a better understanding of personal data and protection, the duties of data handlers and processors, technical and organizational measures which are available or which they are obliged to apply in order to protect personal data of the citizens of Serbia.

(The Guide published in March 2016)

GUIDE A GUIDE FOR AUTHORITIES

PERSONAL DATA PROTECTION

3.3.2. GDPR

An extensive reform of personal data protection rules in the EU was concluded in 2016 by adopting the General Data Protection Regulation (GDPR).[94] The Regulation came into force on 24 May 2016 while its application begins on 25 May 2018, when the Directive 95/46 ceases to apply.[95] The provisions of the GDPR essentially introduce new, more stringent rules for data processors and handlers, which would lead to revision of business models of many companies. The territorial application of the GDPR is extended in comparison to the 1995 Directive, so it also applies to the processing of data of EU citizens by companies outside the Union.

Other major novelties compared to the existing Directive include, among else, the requirement that data processing consent be explicit; new obligations for data processors and handlers; regulation of rights of data portability; right to be forgotten; regulation of the instruments of integrated protection (privacy by design) and offered protection (privacy by default); obligation to conduct privacy impact assessments. Penalties for non-compliance with GDPR provisions are significant: up to 4% of the total annual turnover (not only in the EU, but worldwide).

3.3.3. THE FUTURE OF THE UNIQUE CITIZEN NUMBER

RECOMMENDATIONS

Compromised but intrusive system of assigning each person a unique citizen number should be replaced by a system of randomly generated personal numbers that do not contain personal data. The Central Register of Mandatory Social Security has already established such a system by assigning a Personal Number of Insured Persons (LBOs) containing no personal data; it has already been assigned to almost seven million Serbian citizens and is in use by many state agencies.

By December 2014, the public had learned of the most massive violation of privacy and right to data protection. It was when the SHARE Foundation established that the state Privatization Agency on its website kept an open document containing personal information of 5,190,396 citizens of Serbia - their first and last name, middle name and their Unique Master Citizen Numbers (JMBG).[96] In the ensuing process of inspection conducted by the Commissioner for Public Information and Personal Data Protection, it was determined that the document had been available on the Agency's website for 10 months and that it had been downloaded "many" times, as the Agency's officials told the Commissioner. It is still difficult to fully grasp the consequences of this case and there seems to be a lack of wider understanding of the seriousness of the incident. This is also proved by the fact that the legal proceedings, initiated on the grounds of violation of privacy and the protection of personal data at the Misdemeanor Court in Belgrade against the responsible officials of the Privatization Agency, were dropped in January 2017 on account of a statute of limitations.[97]

There is no information as to who might have obtained this document, whether it was resold on the black market, but the JMBG is still stored in every citizen record of state agencies, and it is still used as a single verification identifier in establishing identity for schooling, commerce, concluding contracts, registration of residence, opening bank accounts, etc. It seems almost needless to point to possible abuses of unauthorized release of a personal data collection containing data of nearly all adult citizens in Serbia. In the age of global networking, false impersonation in electronic communications - phishing, vishing, smishing, depending on whether it is done by mail, phone, or text messages, is a part of an entire discipline of sociological and criminological research, designated as "social engineering" that relies on the simplicity of engaging in personal communication without physical presence. Knowing at least one piece of personal data of the potential victim is the first step of every social engineering fraud based on confidence. The Unique Master Citizen Number would be a perfect means: it represents data closely associated with the authority of state agencies and authorized personal data handlers in general, while it is compromised in a way that renders the provisions of the Personal Data Protection Law utterly useless.

In addition, it should be noted that the JMBG reveals far more information about citizens than it is needed. This number consists of a series of numerals that determine a person more closely. The first seven digits indicate the day, month and year of birth, while the next two represent the registration area code according to the administrative division in former Yugoslavia at the time when the system was introduced in 1976 (Serbia uses numbers

[94] 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) http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[95] 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 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[96] Unauthorized release of personal data of more than five million citizens of Serbia, SHARE Foundation, December 2014 [in Serbian] http://www.shareconference.net/sh/defense/neovlasceno-objavljeni-podaci-o-licnosti-vise-od-5-miliona-gradana-srbije

[97] Statute of limitations expires for data leak in Agency, TV N1, January 2017 [in Serbian] http://rs.n1info.com/a220880/Vesti/Vesti/Curenje-podataka-iz-Agencije-za-privatizaciju-zastarelo.html

from 70 to 89, with the next decade designating citizens born in Kosovo).[98] This part of the JMBG literally expresses the basic facts about citizen's birth. And, again, the JMBG is an essential part in each citizen's record, it is replicated in endless series of dossiers, both paper and electronic, it is published in open databases of state agencies, challenging the limits of protection prescribed by the Constitution concerning the purposefulness of personal data processing.

It seems, however, that there is a relatively simple solution to this problem. In fact, a unique number made up of random digits that, unlike the JMBG, does not reveal personal information, already exists in Serbia and it is widely used. It is assigned to all citizens and residents who have social insurance on any grounds, like employees, children, spouses or else. According to an incomplete survey, nearly seven million citizens and residents already have a Personal Insurance Number (LBO). The number is issued by the Central Register for Mandatory Social Security, the youngest state administration agency that has been created for the digital environment.[99] The number consists of 11 digits, ten of which are randomly selected, while the last one is a control numeral. It is assigned to every insured person only once, it is permanent and unchanging, and it can be used as a unique identifier of the person. Unlike the citizen master number, LBO has no relation to personal properties of the citizen, it does not reveal any information, and the algorithmic choice eliminates the possibility of wrong assignments.

3.3.4. STATE IT & DATA SYSTEM BACKBONE

The Privatization Agency affair (see subchapter 3.2.3) revealed the scope of risks citizens are exposed to, involving the lack of reliable knowledge of practical and technical conditions for collecting, processing and storing citizens' data. The SHARE Foundation therefore decided to investigate which personal data are collected by public agencies, where they are kept, how they are processed, who has access to the data, and which organizational and technical protection measures are implemented. The research was conducted in 2015 and 2016, and it included six agencies: the Serbian Business Registers Agency (APR), Belgrade Center for Social Work (GCS-RBG), the Central Register for Mandatory Social Insurance (CROSO), the National Health Insurance Fund (RFZO), the National Pension and Disability Insurance Fund (PIO), and the Tax Administration.

The research showed that personal data of Serbian citizens were unnecessarily multiplied, identical data being collected by several institutions. This increases risks of data being inaccurate and outdated, affecting the rights of citizens and the efficiency of agencies. More importantly, multiplying data increases the risk for data security, given that identical data are kept on different servers, under completely different technical and organizational security measures.

Among else, it was found that all analyzed institutions had their own servers and other data storage devices, and that all of these devices were located in Serbia, mainly at the headquarters of the institutions themselves. This means that the agencies do not transfer citizen data abroad, thus securing basic preconditions for data control. On the other hand, however, this also means that they rely solely on their own resources for protection, leaving it largely dependant on the available funds.

All institutions, except for Belgrade Center for Social Work, have a centralized information system, i.e. all data processing devices within an institution (servers, computers) are connected within a unique system, which significantly eases the application of security mechanisms. However, keeping all events within the system, the so-called logs, still poses a challenge to some of the agencies analyzed. A particular problem public institutions are facing is hiring and keeping the level of highly skilled staff responsible for developing and maintaining information systems.

The research showed that the exchange of data between these agencies was carried out through the infrastructure of the Administration for Joint Services of State Bodies, via VPN, that is, outside the usual channels of Internet communication, which is very important for data security.

Despite the positive tendencies observed during this research, it should be emphasized that the analysis was carried out in institutions that are among the best systems nationally, with considerable resources available. In Serbia, however, there are over 11,000 public agencies and branches, with far inferior capacities, which is why the situation in systems selected according to their role in the state, can in no way be considered representative.

3.4. ELECTRONIC BUSINESS REGULATION

Electronic business in Serbia may soon be regulated by a new legislative document. At the beginning of September 2016, the Draft Law on Electronic Document, Electronic Identification and Electronic Trust Services was introduced.[100] This law is intended to replace the two existing laws: the Law on Electronic Signature (RS Official Gazette, No. 135/04) and the Law on Electronic Document (Official Gazette of RS, No. 51/2009).[101]

[98] Law on the introduction of a Unique Master Citizen Number [in Serbian] http://www.paragraf.rs/propisi/zakon _ o _ uvodjenju _ jedinstvenog _ maticnog _ broja _ gradjana.html

[99] Central Register of Mandatory Social Security [in Serbian] http://www.croso.gov.rs/cir/index.php

[100] Draft Law on Electronic Document, Electronic Identification and Electronic Trust Services [in Serbian] http://mtt.gov.rs/download/Nacrt.pdf

[101] Third Meeting of National Assembly Economic Caucus, January 2017 http://www.parlament.gov.rs/Third _ Meeting _ of _ National _ Assembly _ Economic _ Caucus.30843.537.html

The purpose of the future law is to enable businesses to perform faster and more efficiently, reduce operating costs, develop market trust and accelerate the workflow of public authorities and business entities, while facilitating access to services for public and other service users.

The Draft Law certainly intends to further harmonize national regulations with the EU regulation on electronic identification and trust services for electronic transactions, which replaced the 1999 Directive on electronic signatures.

The area that needs to be regulated by the new law in Serbia includes the following concepts: electronic document, electronic identification, trust services, electronic signature and electronic seal, time stamp, electronic registered delivery services, certificate services for website authentication, and electronic systems for storing documents.

Experts agreed in principle that the proposed text provides for modern solutions that would contribute to the advancement of e-business in Serbia, but that there was room for improvement regarding certain provisions rewritten from the existing laws that had never been amended since their adoption. [102]

The public debate closed on 30 September 2016. So far, there has been no information available on deadlines that the Government has for making the final proposal.

[102] Comments on Draft Law on Electronic Document, Electronic Identification and Electronic Trust Services, Naled, January 2017 [in Serbian] http://www.naled-serbia.org/upload/CKEditor/Komentari%20na%20Nacrt%20zakona%20o%20elektronskom%20dokumentu%20potpisu%20i%20uslugama%20od%20poverenja.pdf

4. DIGITAL SECURITY

A seminal plan to combat cybercrime as one of four main priorities of Serbia's government was adopted in 2010 in the form of a document called Information Society Development Strategy in the Republic of Serbia by 2020. The Strategy recommends the following measures:

- Adopt regulations in the field of cyber security, which will further regulate the standards of cyber security, as well as the responsibilities and tasks of individual institutions in this area.
- Establish an institution in the field of cyber security which will perform verification and certification of methods, develop software applications, devices and systems, as well as research and development. This institution should supervise the implementation of cyber security standards in state bodies.
- Establish a national CSIRT (Computer Security Incident Response Team), with the aim to act preventively and to coordinate resolution of online computer security incidents.
- Develop and improve protection against attacks by applying information technology to critical infrastructure systems, which in addition to ICT systems may also be other infrastructure systems that are managed using the ICT, such as the electric power system;
- Further regulate the criteria for defining critical infrastructure for cyber security, the criteria for classification of attacks using information technology against the infrastructure, as opposed to other types of attacks, and also the terms of protection;
- Adopt new and improve the existing solutions in national legislation in order to enable compliance with and a more effective implementation of the Cybercrime Convention.

4.1. IMPLEMENTING THE LAW ON INFORMATION SECURITY

Adopted at the end of January 2016, the Law on Information Security was the first legislative document in this area, regulating standards of protection for information systems that private and public actors are now obligated to adopt. The Law defines the ICT systems of particular national significance as the systems used by state agencies, systems that process sensitive personal data, and those in industries and services of national interest.

In the era of sophisticated technical attacks and the rapid development of cyber weapons,[104] it is of crucial importance for information systems that control critical infrastructure,[105] i.e. water supply or electricity, to comply with an adequate level of protection required by law.

One of the most important instruments of the new Law is the National Center for Prevention of Security Risks in ICT systems (CERT), its primary role being the prevention of attacks and coordination of communication among relevant actors in Serbia and abroad.

The Law prescribes the establishment of special CERT's, which should contribute to the prevention and protection against security risks in information systems within a particular area of business, companies, or groups of companies.

Article 7 of the Law prescribes 28 measures for protection of critical information systems, stipulating a number of measures in accordance with changes in the digital environment or the system itself.

Operators of critical ICT systems are bound to regularly conduct inspection of protection measures and file reports at least once a year. Another obligation of the operator is to notify the Ministry of Trade, Tourism and Telecommunications about incidents which may significantly affect the security of information systems.

The Government of Serbia adopted bylaws needed for the implementation of the Law on Information Security on 17 November 2016, setting the standards of necessary protection measures.

Institutions and companies that manage critical information systems, such as government agencies, electronic communication operators and banks, had to adopt internal documents on information system security by March 2017. Since the last week of November 2016, they are required to report any incidents within the infrastructure of information systems to the Ministry of Trade, Tourism and Telecommunications, the National Bank of Serbia and the national Agency for Electronic Communications and Postal Services (RATEL).

[104] 21st Century Warfare http://www.bbc.co.uk/guides/zq9jmnb

[105] Critical infrastructure http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index _ en.htm

Protection of information and communication systems finally found its place in Serbia's legal system, when the Law on Information Security was passed in early 2016. This guide is intended primarily to Operators of critical ICT systems:

- Executives of ICT system operators must have basic knowledge on the importance of cyber security, especially given the fact that they are responsible for misdemeanor in the case of non-compliance with the provisions of the Law and regulations, and can be legally liable in the event of serious failures.
- Technical experts who are responsible for cyber security of ICT systems of special importance, so each of the 29 protective measures that have to be applied is specifically addressed.
- Heads of legal departments in charge of the development and adoption of security acts no later than 2 March 2017.

(The Guide was published in January 2017)

A GUIDE TO CRITICAL ICT SYSTEMS

CYBER SECURITY

4.2. SHARE CERT FOR ONLINE AND CITIZEN MEDIA

The Law on Information Security defines special centers for prevention of security risks in information and communication systems in various sectors. The first special CERT in Serbia was officially registered by the SHARE Foundation in April 2017, as an organization that deals with the systematic study of legal, social, and technical risks to which human rights are exposed in the new communications environment.

Official award ceremony for the certificate of the registration of SHARE CERT

SHARE CERT monitors and analyzes security threats to online and citizen media infrastructure in Serbia, assists in the identification and prevention of threats, empowers actors to adequately respond to attacks, provides legal assistance in the prosecution of cyber incidents, and maintains communication with relevant institutions.

Among else, activities of SHARE CERT include scientific research, education of the general public, citizen and online media, advocating public policies towards improving the standards of human rights on the Internet as well as cyber security, technical services for information systems, legal and technical analysis of incidents, professional aid in their recovery and processing.

SERVICES THAT SHARE CERT PROVIDES CAN BE DIVIDED INTO THREE CATEGORIES:

- **PREVENTION** is the primary service of SHARE CERT and involves the establishment of preventive measures against attacks on information systems. The main preventive measure is the information system audit by the certified ISO 27001 Auditor, which enables the identification of weaknesses in the system, and a process for their proactive resolution. This service includes advice concerning security systems, detection of risks and mitigation of attack effects on information systems.
- **REACTION** includes fast and accurate response in case of a security incident in an ICT system. SHARE CERT team starts active communication with the administrator of the system that was attacked, in order to reestablish the normal functioning of the system as fast as possible; the team collects digital evidence and restores the protection of system integrity. After that, experts from SHARE CERT conduct a forensic analysis of digital evidence and, if necessary, initiate a legal process.
- **EDUCATION** is closely related to prevention and it consists of a special set of services - training for the various target groups, adapted to fit their specific needs, and dissemination of educational content in various formats which are available to the general public. The educational program is based on many years of experience in this field, as well as on data concerning security incidents in the country and the region.

SHARE CERT consists of experts in various fields: cyber forensic experts, lawyers, organizational and technical experts, journalists, and activists. We cooperate with public authorities, industry representatives, internet and civil activists, and the academic community, in order to develop advanced methods and technologies for cyber security.

GUIDE

CYBER SECURITY BASICS

There are a number of factors that affect whether a system will be safe or not. First of all, there are technological factors, i.e. whether the system is technologically compromised or vulnerable and what is the security level provided by installed devices and programs. Then there are also very important non-technological factors, or certain habits of users. The general rule is that security is not an innate characteristic of digital systems, and certain actions must be taken in order to make the system safe.

During their online activity each user leaves certain traces, a "shadow" which accompanies them as they move through cyberspace. In the digital environment, similar to the non-digital one, these shadows indicate certain characteristics of the owner of the shadow. Analysis of the shadows can give some information that is of importance to attackers who aim to enter the system. The advantage of the digital environment is that users can to some extent control the shape of their shadows, which is the subject of this guide.

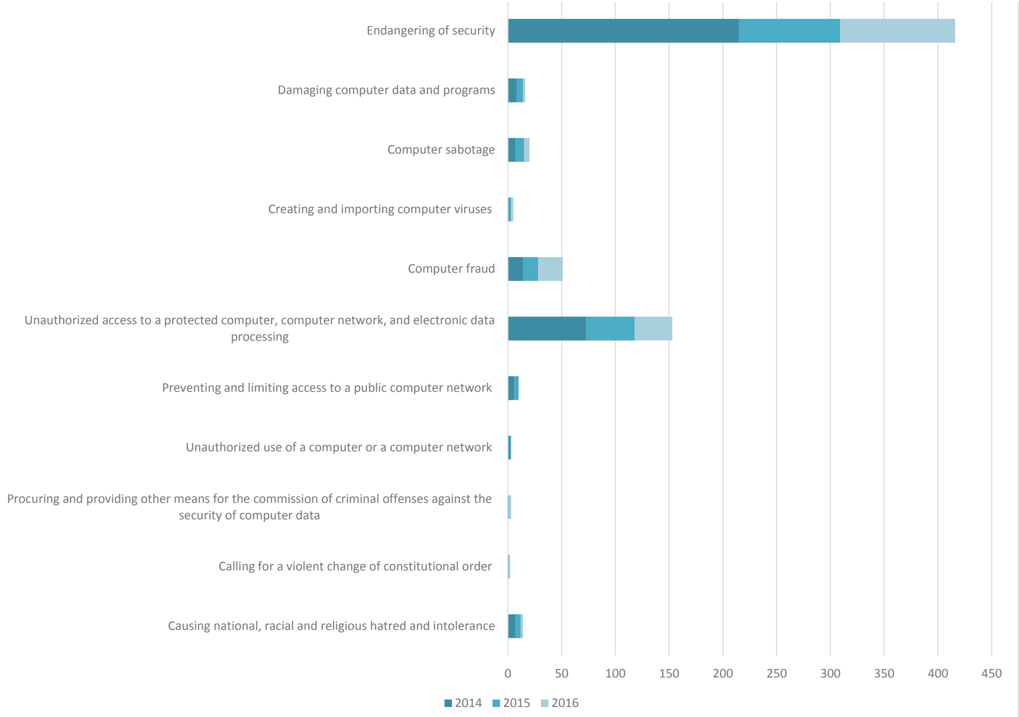
(The Guide was published in March 2015)

4.3. CYBER CRIME: INVESTIGATIONS, CHARGES, ROCEEDINGS

Since cyber crime should be one of the top priorities, we submitted FOI requests to the Public Prosecutor's Office in Belgrade, more precisely its special branch for high-tech crime, in order to collect statistics on the number of criminal charges for certain offenses under the Criminal Code, in the period 2014-2016.

The data refers to cyber crime offenses of in the narrowest sense, but also to other offenses in which a computer or a computer network is used as a means. The most frequent offense by far, at least when prosecution initiated proceedings, is endangering safety. Assuming that the threats were made via social media, the three-year period saw a declining trend, but the number remains relatively high: from 215 criminal charges in 2014 to slightly over one hundred in 2016.

Another cyber crime which stands out by the number of criminal charges is the computer fraud. During 2014 and 2015 prosecution acted 14 times, while in 2016 it took action in 23 cases of computer fraud. The prosecution also often responds to charges for unauthorized access to a protected computer, computer network and electronic data processing, but the number of cases in 2016 was almost two times smaller (35) than in 2014 (74).



Cybercrime statistics 2014-2015

RECOMMENDATIONS

Conduct organized training of judicial officials on cyber attacks in order to increase the effectiveness of responses to cyber attacks against online media. Improve the capacity of state bodies that deal with attacks and other security threats in the online environment, in order to adequately counter the growing number of highly complex forms of threats to freedom of expression.

4.4. PERSONAL AND ORGANIZATIONAL SECURITY

Due to the growing number of cases in which safety of journalists and media organizations was endangered, the SHARE Foundation has developed special guides dedicated to these issues.

Digital safety of journalists is rarely seen from the perspective of their community, that is the circle of people with whom they communicate, the most important ones being the sources and colleagues. It takes only one weak link in the chain of communication in order to put privacy and security at risk. Because of all this, organizational security comes as a priority matter for the media.

IN PRACTICE, MULTIPLE PROBLEMS OF DIGITAL SECURITY WHICH REQUIRE SPECIAL ATTENTION HAVE BEEN IDENTIFIED:

1. Technical intrusions into private communications and access to data
2. Theft and seizure of equipment
3. Electronic communications surveillance conducted by state authorities
4. Social engineering
5. Disabling access to content
6. Endangering safety in the online environment

1. TECHNICAL INTRUSIONS INTO PRIVATE COMMUNICATIONS AND ACCESS TO DATA

General safety risks include unauthorized access through: hacking, insertion of malicious software (malware), use of technology to supervise digital communication for personal purposes, or so-called data leakage due to inadequate protection of an information system.

The main attack points, i.e. the primary targets for attackers: mail servers, devices (computers, mobile phones, tablets), accounts on online platforms (social networks, collaborative tools, chat applications, etc.), carriers of information (physical hard drives, flash memory, cloud platforms – Dropbox or Google Drive).

The main goal of these attacks is to discover information that journalists, bloggers, activists, and media organizations certainly want to protect. The information may involve the following:What you are working on – plans and blueprints of investigative stories or campaigns, documents, records, notes, etc.

- The information that you have – confidential information obtained from sources, potential evidence of misconduct of public officials or private actors (companies, criminals, etc.)
- Who your collaborators are – information about your network of colleagues, sources, editors, etc.
- Your itinerary – information on your position and movement, daily routines, plans to travel abroad, etc.
- Whether you are hiding something – private information that others can abuse.

CONFLICT: privacy and confidentiality in communication v. technical attacks v. digital security of companies that store data.

MEANS OF PROTECTION: internet and telecommunication companies, providers of services in the information society, organizations responsible for management of the Internet (Internet governance), the state, the organization and its IT support, individuals responsible for their own content.

WHO IS RESPONSIBLE: Internet and telecommunication companies, providers of services in the information society, organizations responsible for management of the Internet (Internet governance), the state, the organization and its IT support, individuals responsible for their own content.

2. THEFT AND SEIZURE OF EQUIPMENT

Theft or seizure of equipment by the order of state bodies (police, prosecution, court) is another possible scenario. While police search of newsroom in Serbia is not recorded in practice, the case of portal Klix.ba from neighboring Bosnia and Herzegovina, whose premises was raided by the police, in order to seize and destroy part of the equipment, indicates that this risk still exists.[106] In Serbia, the unauthorized seizure of equipment was recorded when journalists from the investigative portal KRIK tried to ask the Mayor of Belgrade some questions.[107] In case of theft of devices such as a laptop, tablet, phone, or camera, the perpetrator with sufficient technical skills would not have a problem to obtain information which is protected by a weak password. Encryption of hard disk is therefore very important for protection of confidential information, even in the event of device theft.

CONFLICT: protection of journalists' sources v. disabling of reporting.

MEANS OF PROTECTION: advanced Encryption, backups (data backup).

WHO IS RESPONSIBLE: corporations, IT support, individuals for their devices and data.

3. ELECTRONIC COMMUNICATION SURVEILLANCE CONDUCTED BY STATE AUTHORITIES

When working with confidential information, a potential risk is interception of communication by state authorities (police and security services). According to Serbia's legal framework, confidentiality of communication is guaranteed by the Constitution, and this rule can be deviated from only in cases of criminal proceedings or the protection of national security, as prescribed by law and with a court decision. Monitoring by means of video cameras and similar devices in physical space can also represent a critical breach of privacy, although the area of video surveillance is not regulated by existing laws.

It should be noted that there is a lack of control regarding software market for monitoring and interception of electronic communications in Serbia. Private actors can easily get sophisticated equipment and programs necessary for surveillance, since the installation and use of these programs are quite simple.

Surveillance and following are the most common forms of invasion of privacy. However, communications data – the so-called metadata – reveal far more than the content of communication itself. In case of a phone conversation, metadata is the information about the number you dialed, at what time you made the call, how long the conversation lasted, etc. According to the Law on Electronic Communications, which calls this data the retained data, operators are required to keep them for 12 months and make them available to authorized persons in accordance with the law. By carefully combining large amounts of metadata you can easily get a complete digital profile of a certain person: location, daily routines, social network, sources of information, interests, etc. Access to this information represents a very intrusive measure which deviates from the guarantee of confidentiality of communication, so stakeholders in the public and private sectors who keep this data must follow the procedures prescribed by the Law on Protection of Personal Data.

Let us remind of the fact that the Commissioner for Information of Public Importance and Personal Data Protection inspected the operators of

[106] Who ordered search of Klix offices, December 2014 [in Bosnian] http://www.klix.ba/vijesti/bih/ko-su-glavni-akteri-koji-su-naredili-i-odobrili-pretresportala-klix-ba/141230118

[107] Mayor's bodyguards prevented KRIK from asking questions, October 2015 [in Serbian] https://www.krik.rs/obezbedenje-gradonacelnika-sprecilo-krik-da-ma-lom-postavi-pitanja/#sthash.k3u72Mr5.dpuf

mobile and fixed telephony in 2012 and discovered some disturbing facts about illegal access to metadata by state authorities. It was found that in one year and with one provider only, the police had directly accessed the communication data of users more than 270,000 times.[108] Because operators are bound to submit statistics on the number of requests, publicly available data revealed that during 2015 state authorities had a total of 300,845 instances of access with only one operator.

CONFLICT: privacy v. security
MEANS OF PROTECTION: international standards of human rights, watchdog initiative [109]
WHO IS RESPONSIBLE: state, police, secret services, judiciary, electronic communications operators

4. SOCIAL ENGINEERING

Social engineering is another tactic that can be used to collect confidential information from journalists and their sources. It refers to manipulation in order to gather information or to fraudulently access an information system. This is often one of the many steps within the complex plans of fraud. For example, a reporter can receive an e-mail from an address that appears credible with "confidential document content" in the attachment, which actually turns out to be a virus; or emails are sent from fake sources, aiming to find out information from journalists in connection to their work. Anonymity and unverified contact allow that an individual falsely represents themselves as a journalist[110] in order to fulfill their hidden agendas. Due to a number of different circumstances, this can often lead to the abuse of trust (e.g. "leaks" of information from a dissatisfied former colleague), which can cause specific problems.

CONFLICT: trust v. anonymity
MEANS OF PROTECTION: national criminal law, verification of identity (encryption/signing emails)
WHO IS RESPONSIBLE: states, corporations, IT support, individuals

5. DISABLING ACCESS TO CONTENT

In most cases, the security of content published on an online platform depends on the security practices of that particular platform. The most common risk is server flooding with DDoS (Distributed Denial of Service) attacks, i.e. clogging the hosting server on by sending a huge number of access requests at the same time.[111] Another way to undermine the integrity of content is its removal or modification. These attacks are carried out by insertion of a malicious code into an online media site database in order to compromise content (aka. SQL Injection [112]).

A legal way to make specific content somewhat inaccessible is by submitting requests on the basis of the "right to be forgotten" or the procedure for removal of reported content (notice-and-takedown). The right to be forgotten for the time being is practiced on the European Union territory, in accordance with the decision of the European Court of Justice in the case of Google versus Spain. [113] This verdict enables EU citizens to request removal of false or irrelevant information from search services, although only from search results and not from the sites where they are published. Regarding the procedure of content removal upon request, it is usually applied in cases when a request is sent to specific platforms asking them to remove content on some legal grounds (e.g., copyright infringement).

CONFLICT: free access to information v. network architecture
MEANS OF PROTECTION: Budapest Convention on Cybercrime, the national legal framework
WHO IS RESPONSIBLE: Organizations responsible for management of the Internet (Internet Governance), states, corporations, hosting & IT support

6. ENDANGERING SECURITY IN THE ONLINE ENVIRONMENT

Endangering the safety of journalists, which is in the offline world manifested as threats, is gaining momentum on the Internet, especially on social networks, due to anonymity. It is estimated that more than a quarter of cases of threats and intimidation of journalists are carried out online, while female journalists are three times more exposed to verbal violence on the Internet from their male counterparts.[114] Former OSCE Representative for Media Freedom Dunja Mijatovic called on member states to take serious steps towards creating a safer environment for female online journalists.[115] The main objectives of these attacks are intimidation in order to discourage reporting on certain topics, public ridicule, and encouragement or justification for physical attacks against journalists. This is done through open threats, revealing private information such as addresses, names, or photos of family members, hate speech, insults that encourage violence, harassment on social media and the like. When it comes to more subtle tactics, we should mention the degradation of journalists' reputation and the engagement of hackers.

CONFLICT: freedom of expression and anonymity v. personal rights and quality of information
MEANS OF PROTECTION: international human rights standards, national legal framework, self-regulation
WHO IS RESPONSIBLE: internet communities, states, corporations, individuals

[108] Invisible infrastructures: Surveillance Architecture, SHARE Labs, June 2015 https://labs.rs/en/invisible-infrastructures-surveillance-achitecture/

[109] The International Principles on the Application of Human Rights to Communications Surveillance, drafted by a global coalition of civil society, privacy and technology experts in 2013, have been endorsed by over 600 organizations worldwide, the SHARE Foundation included https://en.necessaryandproportionate.org/

[110] In the case of journalist Dragana Peco, unknown person(s) sent FOI requests under her name, from a fake email account [in Serbian] http://www.cins.rs/srpski/news/article/saopstenje-za-javnost-783

[111] Understanding DDoS http://www.digitalattackmap.com/understanding-ddos

[112] SQL Injection attacks https://www.acunetix.com/websitesecurity/sql-injection

[113] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN

[114] Violence and Harassment against Women in the News Media: A Global Picture, IWMF http://www.iwmf.org/intimidation-threats-and-abuse/

[115] Communiqué on the growing safety threat to female journalists online, OSCE http://www.osce.org/fom/139186?download=true

Cyber attacks on online media and journalists are becoming more common in Serbia. Web portals have been targets of DDoS attacks which prevent access to their content, and also the attacks that affect the integrity of the database. These cases have not yet been solved. Journalists are faced with the challenges of social engineering, seizure and online identity theft, and unauthorized access to private communication. Civic journalists that participate in public debates are affected by manipulation of public opinion, intimidation by anonymous threats, in addition to the annoying double standards of prosecution when it comes to cases when freedom of expression is possibly exceeded. In order to better explain and present these problems, we will assess the current position of online media and journalists in the digital environment, taking into account the fact that they keep particularly confidential and sensitive information not only on their devices, but also across the network. This report will therefore pay special attention to digital risks, for example loss or disclosure of information, mechanisms for reducing and avoiding risk, responsible actors, and relationship between opposing values (for example privacy v. security).

(The Guide was published in October 2015)

GUIDE

THROUGH THE RISKS AND MECHANISMS OF PROTECTING THE INDEPENDENCE AND SECURITY OF ONLINE MEDIA

WALKING ON THE DIGITAL EDGE

4.5. TECHNICAL MONITORING: SELECTED CASES

In 2016 the number of registered technical attacks against online media significantly reduced in comparison to the previous two years. The drop is certainly a consequence of further improvement of information system protection by online media and an increasing use of other forms of pressure beside cyber attacks.

The cases where the SHARE Foundation technical team was involved in 2016 illustrate the general climate in the area of internet security.

1. CASE I

TYPE OF ATTACK: Defacement of investigative media website

TIME OF RESTORATION: After three hours the domain was brought online in read-only version from a backup. It took four days to establish the full functionality of the site, having enabled editing and publishing of new articles.

DESCRIPTION: The layout of the site was changed on 26/05/2016, a few minutes after 11 o'clock at night. Attacker accessed site from IP address 185.67.177.228 as an administrator and using the system for dynamic content management, changed the look of the site by placing images.

Only one minute passed from the first visit from IP address used for attack, until the attacker accessed the site with administrative credentials, which could mean that the attacker used a software error to steal the password or launch the attack. It is possible that the administrator password was easy to guess, or that someone from the organization, intentionally or unintentionally, had given the password to the attacker. Before the attack, there were no indications that the site had security issues.

Inspection of SHA1 passwords, which are kept in the database, showed that some passwords were used repeatedly to access the site through administrator (super-admin) functions. One password is used two, and the other three times.

SOLUTION: The first step included the removal of the altered site. It was then returned to read-only mode from a backup that was not infected by the malicious code. Since the system makes backup two hours after midnight, the last backup was made approximately 24 hours before the attack.

Given the fact that the attacker had complete access to the system, it was presumed that all passwords were compromised, including those used for accessing the database. These passwords were changed immediately, while others were generated before returning the site to its full functionality (read-write). When the site was fully restored, administrators continued the research to find the exact vector that allowed access to administrative privileges.

RECOMMENDATIONS: Full access for reading and editing (read-write) should be possible only in directories that are necessary for site operations. Full access to other directories should be disabled. Running PHP scripts in those directories should not be possible. Protocols for authentication of SSL/TLS should be mandatory for all access as well as user and administrator access. Accreditation for all sites must be changed, unnecessary accounts should be removed, and weak passwords should be changed.

2. CASE II

TYPE OF ATTACK:DDoS attack against an investigative media website

TIME OF RESTORATION: Due to the type of content, it took an hour to bring back the site online on a new server.

DESCRIPTION: The attack was launched on 02/09/2016, by a huge amount of requests for site access. At the time of the attack, the administrator was preparing the migration of content to a new and better server. As for sources of the requests, logs shows that a number of IP addresses came from all over the world, mostly from the US, which suggests that attack came from a so called bot network, a group of infected devices.

On the current server, logging via a standard port for SSH (TCP port 22) was not possible, but the site used a non-standard port for SSH access to the server, which is a positive safety practice. Logging was enabled only for eight IP addresses, which is why it was not possible to log in with root access. This means that the logging was enabled only at the user level, while the persons authorized for root access should log in as regular users and then make a specific command (switch user) to change to root access.

All passwords were random, with 16 characters. Fail2ban service was implemented on the server for keeping track of all wrong logins and it denies access to users who enter a wrong password three times in a row.

The organization was planning to migrate the site to a new server on the very day when the attack began. After the attack, the administrator decided to start migration immediately, which is why the site was inaccessible for about an hour. The attack lasted 20 minutes, and caused very slow access to the site.

Given the circumstances, it is unlikely that there had been an incursion into the server, because all safety standards were met. The server log generated during the attack was very big (130 GB) and the analysis of its segments determined that IP requests were coming from all over the world, mostly from the United States.

SOLUTION: After migration, the site was transferred to a new server with fresh hardware and software. All standard technical protection measures were established, including mitigation of DDoS attacks in two layers – server settings which block any IP address that sends more than 10 requests in 5 seconds, and mitigation of hosting provider (Hetzner), which uses a special filter (firewall) that reduces DDoS and other types of server attacks.

RECOMMENDATION: Implementation of mechanism for mitigation of DDoS attacks. Setting up a server to block persistent requests after a certain period of time.

3. CASE III

TYPE OF ATTACK: DoS/DDoS attack on media website

TIME OF RESTORATION: A few hours

DESCRIPTION: At the very end of the election campaign, on 21/04/2016 a media website from Sandzak area was under the attack. The attack started around 17 pm and lasted several hours, during which time the site was unavailable. After the end of the attack, the functionality of the site was normalized and the site was available again.

At the time of the attack, backup settings at the server that hosts the website was disabled, which is the reason that log files were automatically deleted after server reboot. After the attack, the server was restarted and the log files were deleted permanently, which is why it was not possible to determine the precise details of the attack and its source.

SOLUTION: The incident was reported after the attack, when the site was fully functional. Due to the lack of server logs, it was not possible to do a more detailed analysis.

RECOMMENDATION: Implementation of mechanisms for mitigation of DDoS attacks. Setting up the server to block persistent requests after a certain time. Establishment of a mechanism for site and server log backup on a regular, daily basis.

4. CASE IV

VTYPE OF ATTACK: DoS attack on NGO website.

TIME OF RESTORATION: A few hours

DESCRIPTION: an NGO from Belgrade reported that the site was under attack on 29/02/2016. A few days earlier, the organization had received a notice from its hosting provider that the access to the site was limited due to the large number of requests, which suggested that site was under DoS attack.

The hosting provider system for traffic monitoring recorded increased website activity from an IP address (132.150.226.76) registered with Telenor in Norway. In order to prevent a larger scale attack, the system automatically disabled access to the site and informed the organization. At the same time, the Twitter account @SRBnetw0rk posted two tweets which were connected to the attack on the website of the organization.

SOLUTION: The first step was to improve the hosting package so that it included a larger monthly data flow. A service for mitigation of DoS/DDos attack was activated. Server logs were reviewed and it was determined that the IP address from which the attack was made was registered on the network of Telenor in Norway.

RECOMMENDATION: Implementation of a mechanism for mitigation of DDoS attacks. Setting up the server to block persistent requests after a certain time.

Work of journalists and civil society organizations in the community which are expected to timely and accurately inform the public and public interest in the digital age is not possible without appropriate technical protection of sensitive data. From internal operations, organizational plans and communications with confidential sources, to online content, the whole information system of the media and civil society organizations is made up from data whose integrity is necessary to preserve. Network administrators and webmasters have joined journalists and activists on the frontline in the fight for public interest.

This guide is intended for information systems technical staff in media and civil society organizations, who need to improve their knowledge about protection of hardware and software.

(The Guide was published in October 2015)

GUIDE

ORGANIZATIONS AND THEIR SAFETY IN DIGITAL ENVIRONMENT

HOW TO PRESERVE PRIVACY AND CONFIDENTIALITY OF DIGITAL COMMUNICATION

5. OPEN ACCESS TO KNOWLEDGE

5.1. INTRODUCING OPEN DATA IN SERBIA

In accordance with the Strategy for e-Government Development of the Republic of Serbia 2015-2018, and the Action Plan for the Implementation of the Strategy 2015-2016, in 2016 the Open Data Working Group was established. The SHARE Foundation has two representatives in the working group's subgroup for legal issues, whose task is to analyze the legal framework of the Republic of Serbia in the context of data disclosure and to propose future legislative solutions in this area. In this regard, particular focus is on the alignment with the EU Re-use Directive 2013 (Public Sector Information Directive, PSI Directive). [116]

Given that the positive law of the Republic of Serbia does not yet know of the concept of open data, it is necessary to define and put it in an appropriate context. Namely, "open data", "data disclosure", and "the right to reuse information" are closely related and interdependent concepts.

Open data have a similar source as "public information": both concepts are based on the requirement that the work of state bodies should be transparent and that the public should have access to documents which state bodies produce in their work (apart from the clearly defined exceptions, such as the national security, the interest of judicial and other proceedings, etc.). However, open data, as opposed to public information, have certain peculiarities because, apart from transparency, the emphasis is on the information that the public can use for other purposes, different from the ones they had when the relevant authorities collected or produced them ("further commercial or non-commercial use"). Therefore, open data have specific qualities: they are in an open and machine-readable form, suitable for further use, which does not have to be the case with public information.

Since the Open Data Movement is based on ideas of transparency and benefit for the private sector, there is a request for states to proactively disclose their data, i.e. to publish the information they collect in their work in open formats. Publicly available information can thus be used by any person in the private or public sector. However, in the EU at this moment there are no regulations prescribing the common minimum of rules that member states must comply with when actively opening data, nor rules as to which area, type, and scope of data must be open or disclosed. In that sense, each member state has the right to regulate this issue by its national legislation. If a state were to proactively disclose all the information in an open form, the imperative of transparency would be fully met. However, in reality, the first goal is to secure the right for the private sector to request from the state certain data in line with their specific needs. This is the field of "the right to reuse information", where the state is acts passively, i.e. only upon request.

The right to reuse information presupposes that citizens have the right to address the relevant authority and receive specific information of appropriate quality, or open data - if these data are already publicly available, the citizen can access them without submitting a special request. It could be said that the right to reuse information is one of the means of pressure on the state to open its data, i.e. disclose them in an open form, respecting the principles of transparency. In the European law, there are rules on how the bodies of member states have to act if they receive a request from a single person (physical or legal) for certain open data, which are in fact the rules of the PSI Directive.

Thus, the proactive aspect of open data, i.e. public disclosure of certain open data sets, implies a set of rules where there is no minimum requirement in the EU, or only one provision of the PSI Directive; while a passive aspect, i.e. the provision of open data for reuse only upon a specific request, implies another set of rules (the PSI Directive applies).

5.1.1. LAW ON ELECTRONIC ADMINISTRATION

The regulation of public administration bodies' obligation to disclose data sets in an open form is closely related to the establishment and management of electronic data and documents, i.e. their diffusion through electronic communication within electronic administration (e-governance). This matter should be covered by a new law that would regulate electronic administration in the Republic of Serbia.

Given that data disclosure necessarily implies electronic communication that would have to comply with the e-governance regulations, the relevant law seems to provide more than an adequate context for regulating the State's obligation to publish certain data sets in an open form.

As the draft law on electronic administration is in an advanced phase of completion, in cooperation with the working group, it is necessary to reach a common understanding of the way in which the provisions on the open data could be covered. At the end of 2016, the legal subgroup of the Open Data Working Group prepared a proposal for legal provisions in this matter, which are to be presented at the next meeting of the Working Group on the law on electronic administration.

5.1.2. THE LAW ON FREE ACCESS TO PUBLIC INFORMATION

The Open Data Working Group assumed the position that the best solution for the implementation of the PSI Directive would be through appropriate amendments to the Law on free Access to Information of Public Importance. The position was based on research by the SHARE Foundation within the working group, which also concerned the analysis of the PSI Directive application in the EU.

[116] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:02003L0098-20130717

Namely, the 2003 PSI Directive did not oblige member states to disclose data for reuse nor did it provide for a general regimen of access to public information. The amendments to the Directive made in 2013 introduced the obligation to disclose data for reuse, in accordance with the requirements of the Directive itself, and extended the scope of documents to which the Directive relates. At the time of the adoption of the Directive, member states were at a different regulatory level regarding the concept of reuse, some already had national laws, and some introduced reuse only to comply with the Directive. There was also a difference among member states in that some associated the right to reuse with the right to free access to public information, while some had no such clear link, which caused legal uncertainty. The differences in the level of development, the state of affairs and the regimen of national regulations have led to the implementation of the rules of the Directive in various ways:

- Adoption or amendment of existing laws and other regulations that already regulate the obligation to disclose information for reuse.
- Amendment of existing laws on free access to public information (or similar laws) in order to add the obligation to disclose information for reuse in the appropriate format.

There are no legal provisions in Serbia banning the disclosure of information for reuse upon request, but neither are there provisions that enable reuse. The solution of this issue could, in principle, be found among the two main directions assumed by EU member states. At this moment there seem to be enough justifiable reasons to introduce disclosing data for reuse into Serbia's legal framework through the already established rules on free access to public information.

In this respect, it is important to note that movements advocating open government data (OGD) and free access to public information (right-to-information, RTI) have a lot of similarities, but also some differences. The differences are mostly historical – they existed during the emergence of both movements but they are now fading out. Namely, the right to information movement is historically based on the right of citizens to be informed, that is on the idea that the state collects and retains information for the benefit of citizens rather than its own (ideologically driven), while the movement for opening data for reuse puts the emphasis on the technological use of such data for further use, with the aim of innovation and economic progress, while the state accountability and transparency are of secondary importance (technologically driven). [117]

However, authors and professionals mainly hold that the similarities are much more substantial and that, although they do not coincide entirely, both concepts have such a large and significant cross-section that it makes sense to regulate them together. Hence, they can be interpreted in the sense of complementarity, not mutual exclusion.

[117] Yannoukakoua A. & Araka I., Access to Government Information: Right to Information and Open Government Data Synergy http://www.sciencedirect.com/science/article/pii/S187704281404018X

Similarities are first apparent in the identical requests the advocates of both rights pose: transparency of state bodies and freedom of access to all information in their possession, except for the data exempted under a special regime. Advocates of the right to re-use open data may be able to rely on the already developed awareness of the importance of transparent state work, while on the other hand, advocates of the right to free access could benefit if the quality of information increases under the pressure of re-use requests, due to the fact that the requests for free use are in principle more detailed and more specific.[118] In other words, the already established right to free access fulfills its purpose only if the information provided is accurate and clear. Unfortunately, this is often not the case because state authorities themselves do not collect and maintain data properly, information is neither systematized nor verified, and it is not uncommon for authorities to have duplicate information that does not match. The basically open data philosophy could be a motive for state authorities to address these issues, which they have already encountered when applying the law on free access to public information.

In addition, by parallel action and upon requests for free access and re-use, civil servants would develop knowledge and skills in the field of transparent e-government, which would indirectly contribute to improvement in some other areas, the most important of which is competent handling of personal data.

In Serbia's case, what goes in favor of regulating open data within the Law on Free Access to Information of Public Importance is that this Law has been in force for four years and that state authority, professionals and citizens are well acquainted with the rights this Law regulates. Due to the quite high standards of processing the requests for free access to information which are achieved above all thanks to the Commissioner for Public Information and Personal Data Protection, there should be no danger, that professionals are wary of, that the focus of state agencies might slip into the technical aspect of data disclosure, instead of the essential requirement of transparency.[119] On the contrary, the introduction of additional requirements that information be delivered in an appropriate format and available for reuse, may in fact positively influence the maintenance of high standards, with due care when the nature of open data so requires.

Regulating the right to free access to open data within the already existing rules on free access to public information is not without a challenge, but if carefully planned, it can significantly contribute to the favorable development and effective practical application of both rights, and even bring Serbia among more prominent countries in this respect world-wide, especially since open data is a new and challenging topic for most countries.[120]

[118] WWW Foundation Blog, Open data + Right to Information = Right to Data http://webfoundation.org/2015/06/open-data-right-to-information-right-to-data/

[119] Janssen, K., Open Government Data and the Right to Information: Opportunities and Obstacles http://ci-journal.net/index.php/ciej/article/view/952/954

[120] Open Data Barometer http://opendatabarometer.org/3rdEdition/report/; Freedominfo.org, http://www.freedominfo.org/2016/04/open-data-barometer-readslow-and-steady-study-says

RECOMMENDATIONS

It is necessary to amend the legal framework that regulates access to information of public importance so that open data could be regulated in Serbia, and in accordance with that, start opening data sets. Education of employees in state bodies in terms of opening data is also necessary, above all on a technical level, so that the data could be published in a machine-readable format and fulfill other conditions for processing and analysis.

5.2. THE RIGHTS OF INTELLECTUAL PROPERTY

5.2.1. STRATEGY FOR INTELLECTUAL PROPERTY

The Draft of the Intellectual Property Strategy 2016-2020 was proposed by the Ministry of Education, Science and Technological Development to the Government's Economic and Finance Committee, and the open call for public debate was issued on 3 November 2016, but with no information as to who and when participated in drafting the proposal.

The SHARE Foundation invited the libraries, the IT community, the creative sector, civil society organizations, and other stakeholders, to join the preparation of comments on the proposed strategy, warning the community of the non-transparency of the process.

Putting comments together was done in less than seven working days, and the final version was supported by 29 organizations. The overall conclusion of the comments suggests that the proposal of the strategy was made without consultation with public and private actors whose businesses would be directly affected. Some of the solutions from the proposal are in collision with the constitutional and legal framework of the Republic of Serbia, and largely digress from the path of harmonization of the domestic legal framework with the European acquis.

The proposed strategic text ignores the entire range of activities and principles of public interest, such as free access to knowledge and common heritage, freedom of expression in an online environment, information privacy and innovation, creative industries and IT entrepreneurship. The authors of the proposal promote measures to protect intellectual property that could endanger the constitution and the laws protecting citizens' rights, and undermine the principles of the free market. Not taking into account the nature of Internet business nor the technical capacities to carry out the proposed measures, the proposal potentially jeopardizes the operations of information society service providers, announcing a flood of requests to courts. Disputable measures proposed by this document include blocking and filtering websites, deleting domains, creating a "database of suspects", all of which is in direct opposition to domestic and European legal frameworks. Implementing such measures does not reflect the experience of developed countries or relevant research, while the costs of applying and maintaining the proposed measures represents an additional financial burden for Internet providers, which would end up being paid by the citizens of Serbia.

Concluding that if this Strategy Proposal were to be adopted and implemented, the Internet in Serbia would never be the same, the SHARE Foundation and civil society organizations have estimated that the proposed document directly pushes Serbia into a regime of non-compliance with legislative standards of the European Union. Furthermore, the proposed measures are unnecessarily complicated and costly, with little chance of success.

RECOMMENDATIONS

Amendments to legislation on copyright and similar rights need to redefine exceptions and limitations, i.e. the concept of fair use of intellectual property without acquiring consent of the rights holder or paying fees for use, with the goal of establishing the balance between the protection of intellectual property rights and other important rights and interests, such as freedom of expression, cultural rights, right to education etc.

5.2.2. COPYRIGHT AND FREE USE

New technologies have allowed radical changes in production, storage, and distribution of information. Digitization of content stored on traditional, analogue carriers is particularly important for acquiring access to knowledge in areas of general interest such as education, science, public information, or cultural heritage. The beginning of the digitization process is primarily related to the limits of copyright, i.e. the definition of the private and public domain in terms of copyright.

At the end of 2015, the SHARE Foundation, in cooperation with the Belgrade office of the Heinrich Boll Foundation, started the preliminary phase of the project "Legal screening and development of online tools in line with the public domain, in cooperation with the National Library of Serbia (NBS)". After a series of meetings and discussions with representatives of the administration and members of individual organizational units at the National Library, the legal issues in the process of digitization were methodologically listed. The NBS experts accepted this document as an annex to the Memorandum of Understanding signed by the National Library of Serbia, the SHARE Foundation and the Heinrich Boll Foundation - Representative Office in Belgrade.

The project started in July 2016 when complex research was conducted in the area of free content in NBS. The research specifically deals with the question of whether or not the work is in the public domain; whether there is any possibility of using exceptions provided in the Copyright and Related Rights Law; how the license is obtained; how to apply special rules, if the author is unknown, in order to release the material and provide free access to knowledge.

Based on research results, it was proposed that the optimal solution would be to create a copyright guide and an online tool that analyzes the status of work, pointing out the legal exceptions that can be applied to the use of work depending on the user's needs (see section 5.6).

The Guide "Free Use of Copyrights", is intended for institutions of culture, the creative industry, the media and the general public, and contains further clarifications on the possibilities for free use of copyright, in accordance with the exceptions provided for by the domestic law and relevant international conventions. The manual clarifies the legal definitions, types of rights and exceptions, as well as the use of copyrighted work that is in the public domain, therefore free to use without the author's permission and fees. Like other SHARE Foundation guides, this one is also publicly available.

SHARE Foundation's Program Director Djordje Krivokapic and lawyer Jelena Adamovic held workshops for staff of the National Library of Serbia in Belgrade, and also for librarians in southern Serbia at the National Library "Stevan Sremac" in Nis. The workshop included talks on technical innovations, digitization and copyright, as well as free use without infringing copyright.

National Library of Serbia in Belgrade

National library "Stevan Sremac" in Nis

A COPYRIGHT GUIDE

FREE USE OF COPYRIGHTED WORKS

Digital communications technologies have opened up not only access to almost infinite amounts of content but also the ability to create new content ourselves and process the existing one. In the light of the speed of exchange of content and the development of remix culture, Internet users often do not take into account whether photographs, video footage, or texts are copyrighted, or whether and to what extent the right to use and to process them is limited. And if there are numerous exceptions in our legal system that allow free use of copyright, it is sometimes not easy to interpret the law in the right way. Independent artists, journalists, scientists, and lecturers often lack knowledge of legal terminology in this area or resources for consulting a legal advisor.

This guide is intended for anyone who wants to learn more about the possibilities for free use of copyright, in accordance with the exceptions provided for by domestic copyright, related rights and relevant international conventions. We will clarify legal definitions, types of rights and restrictions, as well as the use of copyrighted works that are in the public domain, therefore free to use without the author's permission and compulsory fees.

(Guide published in March 2017)

5.2.3. COPYRIGHT CALCULATOR

The regulatory framework that protects copyright from unauthorized use is a complex barrier to free access to knowledge and free flow of ideas and information in an online environment. Therefore, the technical team of the SHARE Foundation has created a digital community information tool on the criteria for free use and legal exemptions in cases where the work is not in the public domain. The tool is interactive and easy to use: www.copyright-calculator.rs.Developed on the basis of a legal analysis and research in the National Library, the "calculator" works as a quiz guiding the user through the legal copyright labyrinth, providing specific answers to possible doubts when using an author's work. The issue year, for example, answers the question of whether legal protection has expired, or whether the act has entered the public domain. The dilemma on authorship leads to clarification of the legal treatment of a work whose author is unknown. Practical examples illustrate the legal exceptions that allow the specific use of parts of work under full protection, such as education, informing the public, quoting, and the like.

The information tool clarifies the terms and legal criteria for regulating copyright and exceptions, such as the type of work, the user, the purpose, and the manner of use, and is also a modern licensing system for the use of parts under the international creative commons license.

5.2.4. AUTHENTIC INTERPRETATION AGAINST THE PHOTOGRAPH AS AN AUTHOR'S WORK

A series of lawsuits against the media due to unauthorized use of photographs led to an unusual initiative in the Serbian Parliament. Namely, a proposal of "authentic interpretation" of the provisions of the Law on Copyright and Related Rights concerning photography as an author's work, came to the Committee on Constitutional Affairs and Legislation at the beginning of January 2016. The text of the proposed authentic interpretation was aimed at ending copyright protection for every "routine" photo that "appears and is taken over in the electronic form, regardless of whether it is the author's original creation". [123] If it were adopted, such an authentic interpretation would in practice mean that every photo posted on the Internet could be freely used without permission. In the end, the authentic interpretation was rejected by the Committee,[124] but the "defense of photography"[125] certainly remained one of the significant efforts of the professional community and the public in the protection of digital rights during 2016.

The absurdity of the proposed authentic interpretation was already reflected in its explanation, where the existing legal solution was criticized for considering every "routinely" made photograph, even those depicting "a sausage [...], holes in the road" a work of authorship. It is unclear how the writers of the proposal have established the object of photography as a criterion of authorship, or its artistic value, since the law regulates the intended use of the work, regardless of what it contains or what is its quality. The Berne Convention for the Protection of Literary and Artistic Works, ratified by Serbia, stipulates in Article 2, Paragraph 1 that the concept of "literary and artistic works" includes photography and works which use expression similar to that of photography. [126] The Convention, in its Article 9, Paragraph 1 clearly states that the authors of literary and artistic works enjoy the "exclusive right of authorizing the reproduction of these works, in any manner or form".

As for selfies and other personal photos published on social media on a daily basis, their free download and use would not only violate copyright but also the right to privacy and rights to the image. In this respect, it should be emphasized that the practice regarding this issue is not uniform. When they make personal photos publicly available on the Internet, users should bear in mind that anyone can come into their possession and use them for different purposes. No matter if a publicly available photo is considered to be private, the author should know that they have consciously published it on the Internet, and that it is precisely thanks to one's action (by a simple click) that it became publicly available to an unspecified number of people. Depending on the circumstances of each individual case, protection may be required in the event of violation of the rights of a third party, when the image of a person on the photo is used for advertising or other commercial purpose without a license, in which case the person whose image is abused can claim compensation for violation of rights on the image.

An attempt to reform the copyright protection system, considering all the features of online media and the digital environment, using the means of "authentic interpretations" is unacceptable. We believe that the reform of the copyright protection system should be exclusively carried out through amendments to the Law of Copyright and Related Rights, which should be preceded by a serious public debate. At the same time, rights of all actors should enjoy adequate protection, while a fair use of copyright works in public interest (education, science, public information, etc.) should be ensured in accordance with international human rights standards.

[123] "As of Friday Photos to be Excluded from Legal Protection: Anyone could do What They Want with Your Selfie", SHARE Foundation, 2016. [in Serbian] http://www.shareconference.net/sh/defense/od-petka-fotografije-bez-pravne-zastite-sa-vasim-selfijem-svako-ce-moci-da-radi-sta-hoce

[124] "Photographers Win: The Proposal Rejected, Legal Rights Remain", January 2016. [in Serbian] http://www.newsweek.rs/srbija/68987-nije-usvojen-predlog-zakona-fotoreporterima-ostaju-autorska-prava.html

[125] "In the Wake of Photography Defended", SHARE Foundation, 2016. [in Serbian] http://www.shareconference.net/sh/defense/sta-dalje-posle-odbrane-fotografija

[126] The Berne Convention for the Protection of Literary and Artistic Works http://www.wipo.int/treaties/en/text.jsp?file _ id=283698

6.
LABS.RS

6.1. OUR LABORATORY

SHARE Lab, the SHARE Foundation's integral part, deals with analysis and research of data from various technical aspects of social and technological intersection.[127] We explore the invisible paths of electronic immensities, as we strive to better understand new forms of security risks, as well as the risks to privacy and network neutrality. In our research we also try to figure out many phenomena of the digital age, such as the "black boxes" of algorithmic factories.

Using a variety of methods to collect, combine, analyze and visualize data, we have completed a dozen of extensive rounds of research over the past two years, revealing various technical aspects of everyday use of technology - internet history, information wars, mail communication, online political campaigning, "location" of Serbian Internet, and so on.

6.2. INTERNET PRIVACY ATLAS

For investigation of the "Invisible Infrastructure",[128] we used various methods for network topology analysis, data mining and data visualization, in order to create a unique Internet atlas of privacy and transparency, consisting of sets of visual representations and methodologies introduced for mapping, exposing, visualization and independent tracking of various aspects of privacy and transparency on the Internet.

This serial deals with the "life cycle" of one Internet package,[129] a small slice of information that travels through the Web with the help of Internet protocols, and Internet paths of packages[130] leading to the 100 most visited web sites in Serbia. The research also presents the Serbian Internet map[131] – we presented key links and servers that make up the national Internet infrastructure.

We have also presented online trackers,[132] or small programs that collect "digital traces", information about users' movement and behavior online. Based on FOI requests to the Commissioner for Public Information and Personal Data Protection, we obtained statistical data on electronic surveillance and data retention[133] and the ways in which four mobile and fixed telephony operators in Serbia enable the state agencies to have direct access to communication data. Finally, we have examined the permissions [134] we give in exchange for "free" use of mobile apps. Some of the most frequently used applications, especially those owned by Facebook and Google, collect much more data from users than other similar applications (e.g. DuckDuckGo), posing a serious question of users' privacy.

6.3. ELECTIONS

Election campaigns online were also a subject of research by SHARE Lab.[135] Political actors have recognized social and online media as a significant area for building influence and gathering support. During the last two election cycles, in the April 2016 parliamentary elections and the 2017 presidential elections in Serbia, we monitored the engagement of political parties and presidential candidates online, as well as potential violations of digital rights and freedoms.

The 2016 investigation includes texts published by online media covering the parliamentary elections, reactions of public to their texts, and activities of political actors and their followers or opponents on social media. The results showed that parties and political movements that invested more resources in campaigning online on Facebook, managed to achieve their goal and to win seats in the national parliament, at least partially thanks to their increased engagement on social media.

We followed the presidential elections in 2017 from a slightly different angle since, unlike running for parliament, presidential elections imply a much greater interaction between candidates and citizens. In the course of the campaign, Facebook was most extensively used by alter ego of Luka Maksimovic, "Ljubisa Preletacevic Beli", a comic impersonation of an average Serbian politician, managing to attract attention of international press. With over a million recorded interactions, likes and comments on posts at his official Facebook page, "Beli" has led the most active online campaign and won the third place in the presidential race.

[127] Research is available at labs.rs

[128] Understanding Autonomous Systems https://labs.rs/en/as/

[129] The Exciting Life of Internet Packet https://labs.rs/en/packets/

[130] Data Flow https://labs.rs/en/invisible-infrastructures-data-flow/

[131] Internet Map of Serbia https://labs.rs/en/internet-map

[132] Online Trackers https://labs.rs/en/invisible-infrastructures-online-trackers/

[134] Mobile permissions https://labs.rs/en/invisible-infrastructures-mobile-permissions/

[135] Both pieces are part of lab monitoring [in Serbian] https://labs.rs/sr/category/monitoring/

GUIDE

DIGITAL RIGHTS AND INTERNET FREEDOMS IN POLITICAL COMMUNICATION

Social networks, portals, blogs, and other online platforms for user-generated content provide various opportunities for political parties in enabling two-way communication of activists, sympathizers and potential voters.

The development of digital technologies has opened new possibilities for communication, but has also created new forms of violation of fundamental rights to freedom of expression, access to information and sharing, privacy rights, as well as new forms of pressure exerted upon individuals and media organizations. In order to overcome the uncertainty surrounding this kind of technology abuse, we have compiled a handbook with guidelines based on existing legislation, enabling all actors in communication to participate equally in the online political debate, without violating legal and ethical standards, while respecting the basics of Internet culture.

(The Guide published in March 2016)

6.4. FACEBOOK ALGORITHMIC FACTORY

We also examined the implications of immaterial labor, hidden in the algorithmic factories of large internet companies.[136] Everyone with a Facebook account unconsciously works for a company that owns social media by providing daily information about oneself, posting and sharing details that make their digital profile more attractive for monetization or targeted advertising. This invisible and immaterial labor is carried out within the black boxes whose functions we tried to detect.

The research involved mapping and displaying complex and invisible exploitation processes hidden behind the world's largest social media. Facebook research is divided into three parts which describe key processes of algorithmic factories: data collection, storage and algorithmic data processing, as well as behavioral targeting. We have also looked at the silent colonization of lives of Internet users, which Facebook is carrying out assuming an increasingly important role in defining social processes.

[136] There have been five pieces of Facebook research so far https://labs.rs/en/category/facebook-research/

7. SOCIETY IN A NEW ENVIRONMENT

7.1. LABOR RIGHTS AND THE INTERNET

Internet has become an integral part of everyday business. Being tech savvy has become a necessary skill for all employees in today's economy. Labor rights are extending over the digital space and it is very important for companies to control and oversee employees' activities on the web by restricting access to certain websites, monitoring electronic communication and putting policies in place around employee's behavior on social media. In January 2017 the European Court for Human Rights issued the verdict in the case of Barbulescu v. Romania regarding the breach of his right to his private life and correspondence. [137]

The court's opinion in the matter of Barbulescu was that there had been no violation of Article 8 of the European Convention of Human Rights, which guarantees the right on private and family life in case when employers access business communications accounts which employees should use in professional purposes, i.e. for the activities they have been assigned to do. More precisely,[138] according to the court, the employer did not violate Mr. Barbulescu's privacy by checking his business Yahoo messenger account to determine whether he had been doing job tasks during office hours. Even though the stance of the European Court for Human Rights on access to employee's communication accounts (for example business e-mail account) for the sake of checking if employee is doing his job tasks is understandable, it is difficult to find out whether employers in Serbia oversee all employees' communications during office hours, including the correspondence on their private accounts. There are indications that some companies in Serbia use employee monitoring software that allows them to track everything employees do on their work computers. It can be said that there are a lot of questions concerning the legal basis of such measures. However, the cases that the SHARE Foundation has been dealing with on this particular subject were concerning state entities rather than business sector.

As part of its monitoring activities, the SHARE Foundation is following and noting violations of internet freedoms of employees[139] which are usually related to the consequences that employees have to face after posting something online. A typical example illustrating this phenomenon is mobbing of Jasminka Kocijan, a journalist who is involved into a court process against her employer –Tanjug news agency. The journalist's problems started immediately after she made comments on her Facebook account about the event of evacuating snowbound people in Feketic at the beginning of February 2014. It is important to stress out that Kocijan did not post on Facebook while performing journalistic tasks, but while she was on sick leave. Upon her return to work, numerous problems occurred, such as pay reduction and repositioning to lower-ranked positions. Radovan Nenadic, former Trainee of the Higher Court in Belgrade, was fired in July 2015 after a post on social media and a blog where he criticized one of the judges' work, calling him unworthy of the title according to the existing laws. Nenadic asked for protection as a whistleblower, but The Higher Court in Novi Sad passed the verdict according to which Nenadic did not have a whistleblower status, and that in this case the whistleblowing was not in accordance with the Law on Whistleblowers.[140]

Employers are allowed to regulate rules for using social media and devices at workplace but they have to be aware that their internal procedures, policies, working contracts and all other documentation regarding employment and work discipline have to be in accordance with valid legislative framework, more precise with the Constitution and Labour law. Although they are allowed to give instructions to employees about the use of online platforms, they cannot fully limit their guaranteed rights, such as freedom of speech or privacy rights.

Thanks to the Internet, unethical and unacceptable employers' behaviors are now more visible, as we have seen from the previously mentioned examples. Due to the lack of clear directives that should closely regulate user activities online and employers' actions in cases of violation of those directives, in addition to insufficient knowledge of human rights and the digital environment, employers often take hasty steps that can be bad for workers and even illegal. From what we are seeing among workers in both public and private sector, the "chilling effect" is present, which has a negative effect on their digital rights in work environment.

[137] Case of Barbulescu v. Romania (Application no. 61496/08) http://hudoc.echr.coe.int/eng?i=001-159906)

[138] "Can your employer spy on you?" https://sadrzaj.ogledalofirme.com/2017/01/05/itevci-da-li-vas-kompanija-gde-radite-spijunira-2/),

[139] Krivokapic Dj., Perkov B., & Krivokapic, N., Digital rights in the workplace, GISWatch 2016. https://www.giswatch.org/sites/default/files/gw2016-serbia.pdf

[140] The Appellate Court in Novi Sad: Nenadic is not a whistleblower; 021.rs, 2016 http://www.021.rs/story/Novi-Sad/Vesti/158435/Apelacioni-sud-u-Novom-Sadu-Nenadic-nije-uzbunjivac.html#comm

It started as a bitter joke: after cars, workers can now be leased in Serbia. Caused by endless transition and continued unpredictable and unstable market conditions, high unemployment rate and difficult working conditions, bitterness was understandable.

Seriously speaking, leasing has been in practice for decades and it is not necessarily tied to poor economy. In short, it is about renting, or more precisely about getting the right to use goods or services in a specific time frame, while the business conditions are defined through a mediator. Whether it is about services of mercenaries or workers, the mediator is the one who takes care of duties and welfare of the hired ones. This Guide provides a legal framework on labor leasing in Serbia and recommendations for more effective protection of the rights of "rented workers".

(The Guide published in March 2016)

GUIDE

WORKERS ON LEASE

THE RIGHTS OF EMPLOYEES ENGAGED THROUGH THE EMPLOYMENT AGENCY

7.2. COLLABORATIVE ECONOMY

The fusion of technologies which blurs the lines between physical, digital, and biological spheres is a sign of the beginning of the Fourth Industrial Revolution, says Klaus Schwab, the founder of the World Economic Forum.[141] Unlike earlier industrial revolutions, the Fourth Industrial Revolution is developing exponentially, without historical parallel. The radical shift in nearly every industry in every country in the world, with fundamental changes in production, business, and public administration systems, clearly indicates that we have entered uncharted waters.

However, this does not prevent us from enjoying the mix of the most beautiful features of all utopian worlds that humanity has dreamt about. One of them is the sharing economy, or collaborative consumption, the new socio-economic model that has taken off thanks to the technological revolution. [142]

The new model of economic activity, where the customer/user uses their assets more efficiently, provides plenty of opportunity for micro-enterprise business development and lowers the total cost of property ownership. Marketplace is getting flooded with freelancers and workers that choose who to work for and under which conditions, decide on their working hours, and fulfill their needs and obligations on their own. These radical changes in the labor market are influencing financial transactions, which now involve far less intermediaries.

Not possessing anything and having access to everything is a way of life. Is that not just the realization of the vision which guided the social vanguard throughout the history of civilization, as in regular cycles of resistance the enslaved and oppressed were promised human solidarity, equitable prosperity and general welfare?

The digital reincarnation of the Ancient Agora, where free citizens could discuss issues important to the community, was the missing aspect of the unfree labor emancipation – people should participate in creating the value, taking over the means of production and control over their own work.

The constant connection between users and devices they use, suggests not only the future with virtual and augmented reality, but inclusion of virtual activities in the scope of identity. Participation in a networked community is being valued in close interaction with community members, with unlimited geographical or cultural background, based on a complex system of reputation that further undermines traditional social hierarchy.

Many of these changes have already happened, and their impact is felt around the world, regardless of the extent to which local markets manage to catch up. The fact that the new industrial revolution takes place within traditional relations where most people are not familiar with new rules is particularly problematic. People are not able to distinguish when they are in the position of a client, when they are service providers and when they are a product.

At what point does an individual who occasionally provides a particular service becomes an expert and an entity with legally binding obligations? When does social exchange become economical exchange that threatens the previously established market conditions? When does social exchange become a new value eligible for taxation? Should a "shared" place in the car, on the road from Belgrade to Zagreb, be treated as friendly exchange, information society service, or transport service? Who guarantees the quality of service - Internet platforms or participants in transactions? And do the rules of advertising and fair trade apply to them? Who can we contact when we are deceived, manipulated, or unfairly evaluated: the local judiciary or customer service?

The question is how a new social contract will be negotiated when there is still no clear structure of a new society, and the existing regulatory framework is not covering all relations created in the "networked organization of work"?

In order to have access to the labor market, and use all services and products, you need to give up your privacy rights to a certain extent, because the reputation system "feeds on" the information about your past behavior and its algorithmic structure is fully influenced by human prejudices.

Finally, the "sharing economy" is not what it was supposed to be, because corporations are the major player in the process, mediating the exchange between users. It is an economic exchange, whereby consumers pursue utilitarian, rather than social values. Therefore, for the Fourth Industrial Revolution to be successful, utopian enthusiasts need to return to reality and focus on the fundamental issues of a new society. One of the main issues of the 19th and 20th century social movements remains unresolved – is democracy possible without ownership?

7.3. CHILDREN ON THE INTERNET IN SERBIA

The lack of comprehensive and continuous research,[144] along with conceptual and methodological differences, represents a serious challenge in collecting quality data on the behavior of children and young people in Serbia on the Internet, and their exposure to risks in the online environment. There are only a few new scientific surveys that provide a partial view of this sensitive area.

[141] The Fourth Industrial Revolution, January 2016 https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/

[142] European Parliament resolution of 29 October 2015 on new challenges and concepts for the promotion of tourism in Europe http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0391+0+DOC+XML+V0//EN

[143] The Sharing Economy Isn't About Sharing at All, January 2016. https://hbr.org/2015/01/the-sharing-economy-isnt-about-sharing-at-all

[144] The National Youth Strategy for the period from 2015 to 2025, p. 53 http://www.mos.gov.rs/wp-content/uploads/download-manager-files/Nacionalna%20strategija%20za%20mlade%20-%20SR.pdf

On average, children in Serbia begin to use the Internet at the age of eight.[145] Several studies have found that the amount of time children spend online increases significantly as they age. Four out of five young people use the Internet for social media, two thirds are interested in music, and one in four plays online games. The smallest amount of online activities is related to cash transactions. Almost half of young people (45.9%) use the Internet to inform themselves of political events. [146]

The results of the survey "Global Kids Online Serbia" show that 10% of children between the age of 9 to 17 do not possess an internet device of any type (smartphone, tablet, computer), whereas 44% have one device, 32% have two devices, 11% three devices, 2% reported that they have four, and 1% have five devices. [147]

The study shows that the vast majority (95%) of children aged 9–17 go online using a smartphone. A personal computer (PC) or desktop is the second most common device (76%), and nearly two thirds of children access the internet via a laptop or notebook (62%). Children prefer devices they can use exclusively – the devices they own, which are mostly cell phones. Mobile phones are preferred for two additional reasons: going online this way is very easy (wherever they are, they can connect) and there is privacy (they can go online when alone and be the only ones who know what is on their cell phones). They are mostly alone when going online and prefer it that way.

Data from survey conducted by BIRODI (2453 students in the final year of high school) show that only 5.1% of the respondents do not use social media.[148] Almost 35% of respondents who use social media spend from one to two hours a day on it, about a quarter 2 to 4 hours, while 15.8% spend more than 4 hours a day.

Survey results about internet access locations show that the school environment, as one of the most frequent internet access locations, is perceived by young people as not very different from home. This impression correlates with the perception of children's parents who believe that games, music and social media largely occupy children's attention on the Internet, while a much smaller part of internet activities have to do with information and education.[149]

Almost 79% of boys and 63% of girls think that they know more about the internet than their parents. According to Global Kids Online, one third of children aged 9-11, three quarters of the children aged 12-14, and almost all the children aged 15-17 agreed with this claim. Both boys and girls estimate their social skills as highly developed (average score 3.7). Almost 92% of children think that they know what information should be shared with others on the internet, and 94% know how to remove someone from their contact lists, on social networks, for example. Information skills are on the second place (average score 3.2): 85% of children say that they can easily find a website they visited earlier, 78% that they can easily choose the best keywords for internet browsing, while 65% of children can easily check if the information they found on the internet is correct. The skills of mobile device use are in the third place (average score 3.1): 95% of children know how to install an application on a mobile phone, 59% know how to keep track of the expense of using a mobile phone application, while 56% know how to shop via a mobile phone application. Operative skills are in the fourth place (average score 2.8): 88% of children, according to their own statements, know how to save a picture they found on the internet, 77% know to apply privacy rules on social networks – 80% of boys and 74% of girls (73% of all children use social networks every day), 33% of children know to use a program language (40% of boys and 27% of girls), 33% of children know to upload content on YouTube (60% of boys and 32% of girls). Kids evaluate their creative skills as being weakest (average score 2.2) in terms of creating new content and refining existing content on the Internet.

7.4. PROTECTING CHILDREN ONLINE

Analysis of the media market in Serbia from 2015 indicates a trend among young and adult audience (people aged 15-29 and 30-39) who spend less time watching television and more on the Internet.[150] Due to the abandonment of traditional media, regulation of linear television program regarding the exposure of children and young people to harmful content becomes a peripheral issue.

CHILDREN AND FREEDOM OF EXPRESSION - INTERNATIONAL AND DOMESTIC REGULATIONS

Without diminishing the importance of children protection from objective dangers of the Internet, public policies should not limit their rights to freedom of expression,[151] access to knowledge and participation in society.[152]

Although the Universal Declaration of Human Rights[153] and the Interna-

[145] Global Kids Online Serbia

[146] Tomanovic, S. & Stanojevic, D., "Young people in Serbia 2015: The states, perceptions, beliefs and hopes", Friedrich Ebert Stiftung & SeConS, Beograd, 2015. http://library.fes.de/pdf-files/bueros/belgrad/12065.pdf

[147] Popadic, D., Pavlovic, Z., Petrovic, D. & Kuzmanovic, D., "Global kids online Serbia: Balancing between Opportunities and Risks. Results from the Pilot Study", Belgrade: University of Belgrade, 2016 http://blogs.lse.ac.uk/gko/reportserbia/

[148] Media literacy in Serbia, BIRODI, 2013, http://www.birodi.rs/medijska-pismenost-u-srbiji-rezultati-istrazivanja/

[149] Survey on Parental Awareness of Online Child Abuse Risks, UNICEF & Ipsos, 2016 https://drive.google.com/file/d/0B4WVugCwd1buWDlvQkJyaEwxWkU/view

[150] Analysis of the media market in Serbia, Ipsos Strategic Marketing http://www.rra.org.rs/uploads/useruploads/PDF/6529-Analiza%20medijskog%20trzista%20u%20Srbiji%20-%20final.pdf

[151] Article 13: Freedom of Expression https://www.crin.org/en/home/rights/convention/articles/article-13-freedom-expression

[152] S. Livingstone, One in Three: Internet Governance and Children's Rights, LSE http://blogs.lse.ac.uk/mediapolicyproject/2015/11/02/one-in-three-internet-governance-and-childrens-rights

[153] Universal Declaration of Human Rights http://www.poverenik.rs/images/stories/Dokumentacija/54 _ 1dok.pdf

tional Covenant on Civil and Political Rights (Article 19)[154] guarantee the right to freedom of expression of every human being, Article 13 of the UN Convention on the Rights of the Child specifically emphasizes the importance of this right when it comes to minors.[155] The application of this Article shall be considered a clear indicator of the extent to which children are treated as holders of rights, especially in terms of enabling children to express themselves and describe the ways in which their total rights are respected or violated.

The notable abuse of the wide margin for interpretation regarding restricting the right to freedom of expression under key international documents, is usually based on national security interests. In case of children's rights, however, a particularly aggravating circumstance is the patriarchal model in which, even in cases when the society is dedicated to the rights and freedoms of citizens, traditional social attitudes toward children imply the exclusion of minors from participation in public life. The protection of children is the most common excuse for restricting children's civil and political rights.

In the domestic legal framework,[156] the child has the right to have the best possible living conditions needed for its proper and full development, the right to education in accordance with its abilities, needs and preferences, as well as the right to timely obtain all the information it needs to form an opinion. Freedom of information and free access to information are necessary for each of these rights. Parents can restrict these freedoms by exercising parental rights. These freedoms can also be restricted in accordance with the general constitutional principle of freedom of expression, which is consistent with the terms imposed by the UN Convention on the Rights of the Child.

RISKS

Several studies have shown that there is a significant gap between children's testimonies about risks on the Internet and what parents consider Internet risks. For example, research results have shown that the accessibility of inappropriate online content is the biggest parental concern, which is two times stronger than 'traditional' concerns about traffic safety and the potential alcohol or drug abuse.[157] Contacts with strangers on the Internet are the second place on the UNICEF "worry meter" (40.3%).

Research focusing on children's perception of risks reveals that children see online aggression and disturbing content or situations on the Internet as main online risks.[158] Also, the virus infecting the device is rated high among online risks, which is supported by the financial potential for purchasing better equipment or antivirus programs.[159]

7.4.1. PROTECTION AGAINST HARMFUL CONTENT - EUROPEAN FRAMEWORK

The European Directive on Audiovisual Media Services Directive[160] contains specific rules to protect minors from inappropriate on-demand media audiovisual services. The AVMS Directive's general approach also applies to the protection of minors. It is based on the principle that the less control a viewer has, the more specific content could be harmful, which is why more restrictions should apply. The rules in this directive are supplemented by Recommendations from 1998 and 2006 on the protection of minors and human dignity.

The main drawback of the Directive is reflected in its limited applicability to content that is not in an audio-visual format delivered via traditional broadcast media, which is in fact the dominant content that minors today follow through platforms for online exchange. The reform of the Directive on Audiovisual Media Services is trying to tackle this problem and provide for specific rules to protect minors from harmful video content on the Internet, co-regulating the platforms that make content available. The outcome of this process is still uncertain for several reasons, primarily due to the fact that such rules would jeopardize the limits of liability of intermediaries, on which internet business is based, but also due to the fact that the maintenance of existing platforms is extremely resource-demanding.

Advertising aimed at children is subject to specific regulatory mechanisms within the European Union. Directive on unfair commercial practices [161] protects all consumers from unfair advertising practices, paying attention to children who are considered a "particularly vulnerable" group of consumers. Advertising to minors requires special assessment of risks to their development, as well as informing minors what is promotional content, in line with the expected level of media literacy of children.

[154] International Covenant on Civil and Political Rights http://www.bgcentar.org.rs/bgcentar/wp-content/uploads/2013/02/Me%C4%91unarodni-pakt-o-gra%C4%91anskim-i-politi%C4%8Dkim-pravima.pdf

[155] Law on Ratification of the Convention on the Rights of the Child http://www.paragraf.rs/propisi/zakon _ o _ ratifikaciji _ konvencije _ ujedinjenih _ nacija _ o _ pravima _ deteta.html

[156] Family Law, Sl. list RS, no. 18/2005, 72/2011 – dr. Law 6/2015 and Art. 62, 63 and 65`v

[157] Survey on Parental Awareness of Online Child Abuse Risks, UNICEF & Ipsos, 2016, UNICEF & Ipsos, 2016. https://drive.google.com/file/d/0B4WVugCwd1buWDlvQkJyaEwxWkU/view, p. 28

[158] D. Popadic, Z. Pavlovic, D. Petrovic, D. Kuzmanovic, "Global kids online Serbia: Ravnoteža između mogućnosti i rizika. Rezultati pilot studije" (engl.) Beograd, 2016 http://blogs.lse.ac.uk/gko/reportserbia/

[159] UNICEF/Ipsos, p. 40

[160] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32010L0013

[161] Directive 2005/29/Ec Of The European Parliament And Of The Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:32005L0029

7.4.2. PROTECTION AGAINST HARMFUL CONTENT - THE DOMESTIC FRAMEWORK

The home system protection of children on the Internet focused primarily on protection against violence, abuse, and neglect. At the regulatory level, Serbia's Government adopted Regulation on Security and Protection of Children in the Use of Information and Communication Technologies on 30 June 2016[167]. The Regulation stipulates that the Ministry of Trade, Tourism and Telecommunications takes preventive measures for safety and protection of children through information and education, establishing a unique point for advice and complaints related to online safety of children.

The measures that were taken in the period before the adoption of the Regulation are aimed primarily at developing awareness and education on digital violence through research[168], manuals[169], and special communication channels for young people who come into contact with digital violence[170]. The B92 Fund in cooperation with state institutions developed the Net Patrol Service[171] – an online mechanism through which illegal and/or harmful content on the Internet can be safely and anonymously reported. In addition, they created the Click Safely portal for informing the public about the risks and benefits, as well as means of responsible and safe use of information and communication technologies, while online educational tools, games, and quizzes are designed and made available for children and young people[172]. Also, a large number of civil society organizations offered the knowledge base and resources to help children, parents, and teachers oppose the identified risks.

Several laws treat the issue of protecting minors from harmful content, referring to traditional broadcast and print media. These frameworks are applied when media distribute their content on the Internet. However, it should be noted that in the online environment, this role is performed by a number of other actors who do not fall into any of the regulated category, do not reside in the Republic of Serbia, or have specific grounds for exemption from liability. It is these actors that provide the greatest number of online services to minors.

7.4.3. DATA PROTECTION OF CHILDREN IN THE EUROPEAN UNION

One of the most important innovations of the General Regulation on the Protection of Personal Data (GDPR), which will come into force in 2018 in the European Union, is contained the provisions that deal specifically with the protection of personal data of children. The challenge faced by writers of the General Regulation is far from insignificant, since it introduces rules on data protection of generations born in the digital era. Unlike legislators, these children know no social environment other than that which significantly relies on the internet. Statistics estimate that today one in three Internet users in the world is younger than 18, while one in five internet users in the EU is a child.

Disputes over certain solutions are therefore not surprising. Among them is Article 8 (1), which seems to set an excessively high threshold for the opportunity to consent to data processing (EU Member States have the possibility to determine this threshold in the range of 13-16 years). The problem is the fact that GDPR does not introduce mandatory age verification, as well as a very narrow circle of people who can give consent on behalf of the child.

New European regulation is unquestionably a pioneering step focused on privacy. The fact that the General Regulation explicitly recognizes children's rights and their need for special protection, already in the preamble of the text, basically represents a very significant improvement[173]. A significant step forward is the requirement that, in a situation where data processing concerns a child, any information and communication should be expressed so clearly and in a simple language that a child can easily understand.

7.4.4. DATA PROTECTION OF CHILDREN IN THE DOMESTIC LEGAL FRAMEWORK

In the existing law the only provision on the protection of personal data concerning children is based on Article 10[174] Paragraph 6, as well as persons who can provide consent for processing of data about a deceased person, or a child at least "with 15 years of age", which is the applicable age limit when it comes to testaments and working abilities of children. In Paragraph 5, which stipulates who can give consent for personal data processing, children are not mentioned explicitly, but from the formulation "who is not able to consent" it can be assumed that the legislator equally treats their ability to give consent and the capacity to work, including minors into this category.[175]

It is obvious that the legislation of the Republic of Serbia is expected to harmonize with the new framework of General Regulation of the European Union on personal data protection, also when it comes to determining the age limit for giving consent for data processing.

The issue of online development, and the fact that all children of younger ages are exposed to digital technology and constant risks to privacy and protection of personal data, will not be possible to bypass locally either.

Topics relevant to future lawmakers in Serbia will be the establishment of a system of age verification, the issue of teachers and educators as potential carriers of the right to give consent, and abuse of this right in case a parent or guardian does not act in child's best interest. When drafting a new law, professionals and public should pay attention to the relationship of personal data with universal rights and freedoms of the child, such as the right to freedom of expression, the right to access information, the right to participate in decision-making, the right to learn, etc.

7.5. SHARE FOUNDATION: RESEARCH AND PUBLICATIONS

PUBLICATIONS

- Guide XI: A Copyright Guide: Free Use of Copyrighted Works
- Guide X: A Guide to Critical ICT Systems: Sybersecurity
- Guide IX: Workers on Lease - The rights of employees engaged through the employment agency
- Guide VIII: A Guide for Public Agencies – Personal Data Protection
- Guide VII: Digital Rights and Internet Freedom in Political Communication
- Guide VI: Protecting the Confidentiality of Sources: The Legal and Technical Aspects
- Guide V: Organizational Security in the Digital Environment
- Guide IV: Through the Risks and Mechanisms of Protecting the Independence and Security of Online Media: Walking on the Digital Edge
- Guide III: Models for Online Comments
- Guide II: The Legal Position of Online Media in Serbia
- Guide I: Cybersecurity Basics
- Guide: Digital Protectors against Info-intruders (translation into Serbian, published by EDRi)
- Share This Book
- The report on the processing of personal data – Tax Administration
- The report on the processing of personal data – National Health Insurance Fund
- The report on the processing of personal data – Belgrade City Center for Social Work
- The report on the processing of personal data – Central Register for Mandatory Social Insurance
- The report on the processing of personal data – Business Registers Agency
- The report on the processing of personal data – National Pension and Disability Insurance Fund

MONITORING REPORTS

- Monitoring online presidential campaign in 2017 – Trends and tensions on the Internet (14/03/2017)
- Respecting digital rights and freedoms in 2016 (25/01/2017)
- Monitoring of digital rights: a two-month review (21/12/2016)
- Monitoring of digital rights in 2016: Social Conflicts (08/11/2016)
- #elections2016: online campaign pays off (26/04/2016)
- #elections2016: The last day of the campaign (21/04/2016.)
- #elections2016: Zenith of the pre-election campaign (12/04/2016)
- The course of the election campaign on the Internet (05/04/2016)
- Election 2016: Analysis of social networks and online media (26/03/2016)
- SHARE monitors the respect of Internet freedoms and digital rights during the election campaign (24/03/2016)
- Monitoring the state of Internet freedom in Serbia in the last quarter of 2015 (07/04/2016)
- Monitoring Report: increase of verbal abuse on the Internet in Serbia (20/10/2015)
- Digital Rights and Freedoms – the first overview in the 2015 (01/06/2015)
- Internet freedoms and digital rights in Serbia – Monitoring report for the period from 1 August to 31 December 2014 (12/02/2015)
- Analysis of Internet freedoms in Serbia – Monitoring Internet freedoms and digital rights in Serbia, June and July 2014 (08/08/2014)
- Internet remembers everything – Analysis of Internet freedom during an emergency, May 2014 (28/05/2014)
-

7.6. CONFERENCES, INITIATIVES, MEETINGS

7.6.1. DIGITAL SECURITY TALKS

The SHARE Foundation took the opportunity of new Law on Information Security implementation to arrange a series of informal meetings, creating a platform for connecting and strengthening cooperation among key actors of the process – state authorities as decision makers, IT community which implements solutions from Law on Information Security in practice, academic community which is significant because of specific knowledge which it possesses about information security, organizations of civil society, and online media as actors whose activities are influenced by information security.

On Monday, 28 November 2016, the SHARE Foundation held its first Cybersecurity meetup. The topic of the event was the Law on Information Security and its implementation. Participants discussed the importance of this law, as well as bylaws, considering that information security can be threatened in every aspect of the society. Also, it was pointed out that it is necessary to work on increasing the conscience about the importance of information security so that citizens can protect their data themselves.

More than 60 people attended the event, and the speakers were Sava Savic, Assistant Minister for Information Society at the Ministry of Trade, Tourism and Telecommunications, Vladica Tintor, director of Regulatory Agency for Electronic Communications and Postal Services (RATEL), Adel Abusara, Representative of the OSCE mission in Serbia, Slobodan Markovic, Advisor on ICT policy and relations with the internet community in The Serbian National Internet Domain Registry Foundation (RNIDS), and Jovan Sikanja, administrator for security and protection against fraud in the company Limundo.

First Cybersecurity Meetup

Second Cybersecurity was held on 20 February 2017 at Startit Center in Belgrade. The topics of the event were improvement in the use of the Law on Information Security and accompanying bylaws, problematic areas, and roles of the state, economy, and civil sector. The SHARE Foundation presented its guide for ICT systems of particular importance, in order to clarify doubts regarding the application of the law and present best practice regarding information security.

More than 60 people attended the meeting and the speakers were Milan Vojvodic from the Ministry of Trade, Tourism and Telecommunications, Aleksandar Maksimovic – chief specialist lawyer for network and information security Ministry of Interior CERT, Viktor Varga –representative of the Unikom telecom company, Milan Skuloski from the Geneva Center for the Democratic Control of Armed Forces, and Danilo Krivokapic – SHARE Foundation coordinator for privacy and protection of personal data.

The event agenda contained a workshop dedicated to the risks and problems that media face in terms of information security, which was attended by journalists, civil society representatives, and media associations.

The Cybersecurity meetup series is organized by the SHARE Foundation in cooperation with the Ministry of Trade, Tourism and Telecommunications, the eSecurity Association, Startit, and the Informatics Association of Serbia. The next meeting is planned for May 2017.

7.6.2. OSCE CONFERENCE "GAINING A DIGITAL EDGE: FREEDOM OF EXPRESSION"

Conference dedicated to Freedom of expression in the online sphere, organized by the Office of the OSCE Representative on Freedom of the Media, the OSCE Mission to Serbia, the SHARE Foundation, and the Center for Media, Information and Society at the School of Public Policy at Central European University in Budapest, took place in Vienna on 15 and 16 November, and brought together about 120 journalists, media lawyers, government representatives, IT professionals, professors, artists, and human rights defenders from South East and Central Europe. Discussions focused on the challenges and reviews of journalism in the digital environment, as well as regulation in online sphere. This was the fourth conference on media freedom. So far those conferences were held in Kotor (2013), Budapest (2014), and Belgrade (2015).

The conference was opened by Dunja Mijatovic, who was then the OSCE Representative on Freedom of the Media, and who emphasized that without the Internet today, there would be no freedom of expression and media freedom. Pointing to international standards which may limit this freedom, Mijatovic highlited the importance of dialogue on the conflict of interests of national security and public order and interest in the protection of freedom. The audience was also addressed by Peter Burkhard, Head of the OSCE Mission in Serbia, and Desire Kopmels, Ambassador of the Netherlands to the OSCE.

The presentation of Jacob Mchangama, founder and director of the Danish think-tank organization "Justitia", was dedicated to increasing restrictions imposed on the freedoms and rights on the Internet, in the form of censorship, criminalization of expression, and surveillance. This was followed by a panel discussion on a new understanding of journalism ("Re-thinking journalism"), which was attended by professor Natali Helberger from the Law Faculty of the University of Amsterdam, Igor Bozic, executive producer of television N1, Andrew Finkel, member of the Platform for independent journalism P24 from Turkey, and Fredrik Laurin, editor of the Investigative Reporting section at Swedish television SVT.

The representative of the Hermes Center for Transparency and Human Rights in the Digital Environment spoke about the partnership of digital journalism and hackers in public interest, after which conference participants could choose between two panel discussions that were held at the same time – on women in the media, or the rapid growth of immersive journalism. In his next lecture he presented research on the minimization of distrust and political polarization, necessary in order to achieve and strengthen a visionary political debate, and the key role of constructive journalism.

The final part of the first day of the conference consisted of two parallel lectures: "The Page View is a Zombie" by Dejan Nikolic, founder of Content Insights, and "Inside the Facebook Algorithmic Factory" by Vladan Joler, founder of the SHARE Foundation. After that there was a panel discussion on algorithms and new forms of censorship, which was attended by Hussein Deraksan, an independent researcher from Iran, Ben Wagner, director of the Center for Internet and Human Rights of the European University Viadrina from Germany, dr. Radim Polcak, director of the Center for law and technology Masaryk University in the Czech Republic and Lenart Kucic, a reporter from Slovenia.

Second day of the conference "Gaining the digital edge: Freedom of Expression"

On the second day of the conference, the representatives of the OSCE held a panel devoted to the activities of this organization which protect and promote the safety of journalists. Afterwards there were discussions on the regulation of content on the Internet, which were attended by Daniel Baer, US Ambassador to the OSCE, Joe Meknami, Executive Director EDRi network, Marius Dragomir, director of the Center for media, data and society - CEU in Hungary and Djordje Krivokapic, program director of the SHARE Foundation.

Later on, there were four blocks, each with two simultaneous lectures on various topics: the crisis of journalism as a problem of public policy, the importance of net neutrality for freedom of speech, regional opportunities for online journalism, the development of new media business models and establishing cooperation between journalism and art. The final panel was devoted to the state of the media in the Balkans, bringing together researchers, the media, scientists, and representatives of media organizations.

7.6.3. CONFERENCE "EUROPEAN YOUTH CONFERENCE ON INTERNET AS A COMMONS AND THE NEW POLITICS OF COMMONING"

Organized by the Heinrich Boell Foundation, the SHARE Foundation, the Institute for Political Ecology in Zagreb and the Green European Foundation, a youth conference about the Internet as a public good was held in Belgrade19-21 May 2016. During the three days there were more than 20 panels, open discussions and other activities, with over a hundred participants from Serbia and abroad.

The conference was opened by Andreas Polterman, President of the Heinrich Boell Foundation, and an introductory lecture on the principle of open access was given by professor Rainer Kulen from the University of Konstanz, Department of Computer and Information Science in Germany. There was a regional premiere of the documentary "Democracy – Data Fever," in which the authors trace the lobbying and bidding related to a new EU law on the collection and storage of personal data, as well as the consequences of complex legal processes in European and world democracies.

Panel discussion "How Brussels operates and what can we learn from it?"

Brussels procedures were discussed by Julia Reda – MEP from Germany, Asta Helgadotir – a member of the Pirate Party in the Parliament of Iceland, Nevena Ruzic from the Office of the Commissioner for Information of Public Importance and Personal Data Protection of the Republic of Serbia, and Natasa Pirc Musar – a lawyer and former Commissioner for Public Information in Slovenia. The moderator was Djordje Krivokapic, Director of Legal Policy SHARE Foundation.

Later in the program, the participants could choose one out of three panel discussions according to their interest, while the final lecture of Julia Reda and Vedran Horvat, Executive Director of the Institute of Political Ecology, was devoted to the reform of copyright legislation, and the importance of public goods in social and civil development.

On the second day of the conference there were three simultaneous panel discussions on the role of public libraries, archives and museums in the administration of the digital public good, on legal issues concerning intermediaries on the Internet, and public spaces in the era of virtual and augmented reality. It was followed by lectures on art and the public good (Kristian Lukic from the Institute for Flexible Culture and Technology in Novi Sad), challenges and limitations of internet activism (Peter Sunde, one of the founders of the torrent search engine The Pirate Bay), data economics, information on the Internet and the risks to privacy (Gemma Galdon Clavel, director of the organization Eticas Research & Consulting from Barcelona), and data economy outsourcing (Fike Jansen, executive director of the Tactical Tech organization from Berlin). The day ended with a block of panel discussions on various topics related to online collaboration, privacy and programming, while the SHARE Labs research dedicated to algorithmic factories of Facebook was introduced by Vladan Joler, founder of the SHARE Foundation, Kristian Lukic from the Institute for flexible culture and technology from Novi Sad, and Jan Krasni, associate at the SHARE Foundation.

The third day of the conference began with a lecture of Zaneta Hofman, director of the Humboldt Institute for Internet and Society in Berlin on the topic of trust in the institutions and mechanisms of Internet governance, followed by Djordje Krivokapic, director of legal policy of the SHARE Foundation, who delivered a lecture on reputational systems. Zaneta Hofmann and Peter Sunde participated in a panel discussion on self-management of communities on the Internet, after which there was a block of three simultaneous panels on algorithmic decision-making, whistleblowers in the digital age, and sexual and gender rights on the Internet.

A pervasive card game called "DeckLaration" was developed especially for this event, with announcement of winners and prizes at the final event.

7.6.4. MOKRIN: CONSULTATIVE MEETING WITHIN THE PROJECT "PERSONAL DATA IN THE PUBLIC SECTOR: MAPPING PUBLIC DATA PROCESSING INFRASTRUCTURE IN SERBIA"

Within the project "Personal Data in the Public Sector: Mapping Public Data Processing Infrastructure in Serbia", which was supported by USAID JRGA project, the SHARE Foundation organized a two-day consultative meeting in Mokrin, 25-28 February 2016. The meeting was attended by representatives from the following institutions: the office of the Commissioner for Information of Public Importance and Personal Data Protection, the Central Registry of Mandatory Social Insurance, Pension and Disability Insurance Fund, the Center for Social Work Belgrade, Business Registers Agency, Partners for Democratic Change Serbia, JRGA project, and the SHARE Foundation.

On this occasion the SHARE Foundation presented the publication "Guide for authorities: protection of personal data" intended primarily for public authorities, and representatives of the private sector who handle personal data. The aim was to gather participants' comments and objections to the text of the guide, in order to improve it even further.

The guide was created as the result of extensive research on the types of treatment and methods of protection of personal data in the public sector. The study included six state institutions: the Business Registers Agency, the Center for Social Work Belgrade, the Central Registry of Mandatory Social Insurance, the National Health Insurance Fund, the Pension and Disability Insurance Fund, and Tax Administration. As part of the project, the SHARE Foundation set up a special website – www.mojipodaci.rs – which in addition to the electronic version of the Guide, gives an overview of frequently asked questions related to personal data processing, as well as the most common issues of state bodies in this area, and recommendations for their solution.

7.7. TV DOCUMENTARY SERIES "IN THE WEB"

SHARE FOUNDATION, BELGRADE 2017
WRITTEN AND DIRECTED BY Mirko Stojkovic, PhD
EXECUTIVE PRODUCERS: Djordje Krivokapic, PhD; Vladan Joler, PhD
DISTRIBUTION: TBA

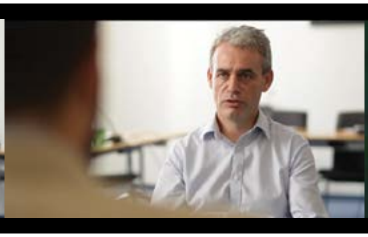
After years of research, conferences, numerous publications and discussions, in 2016 the SHARE Foundation embarked on a popular science and education TV series project, concerned with topics that have been in public focus over the past few years. The stories on internet structure, virtual reality, new media, privacy and electronic surveillance, freedom of expression online, and other, are adapted for an average viewer who has only just set foot into the world of digital technologies. At the same time,

Vladan Joler, Ana Martinoli and Djordje Krivokapic, speakers and editors of the TV series "In the network" the series addresses viewers from private and public sectors for whom the online environment has become daily work space, with all the risks and possibilities the internet has introduced.

The themes are covered in 10 episodes, giving the historical view of technological development, popular culture, global and national trends, combined into a framework for understanding each of the selected phenomena of the digital age. There are interviews with national and international experts, activists, and authors, such as Julia Reda – MEP, Joe Mcnamee – executive director of the European Digital Rights (EDRi) association, Dunja Mijatovic – former OSCE Representative on Freedom of the Media, Dean Starkman – Pulitzer Prize-winning journalist and author, Peter Sunde – co-founder of The Pirate Bay search engine, and dozens of others.

The program is intended for broadcasting on a TV with national frequency combined with various additional multimedia content comprising a single, free, interactive knowledge base. This platform will include publications, research, visual and video material, and SHARE Foundation's educational tools, offering to TV viewers more clarification, information, and detailed analysis. This knowledge base intended for experts, policy and decision makers is unique in the region.

Caroline Bannock, Guardian


Joe McNamee, European Digital Rights (EDRi)

Asta Helgadóttir, Icelandic Pirate Party

SSERIES SYNOPSIS

EPISODE 1 AND 2 - "COMMUNICATION"

Despite the fact that each generation of human civilization is confident in its exceptionality, certain that many things happen suddenly and for the first time in history, that usually is not the case. Sometimes trends last for thousands of years only to materialize at certain stages of technical progress. The time needed for various preconditions to be met in before the decisive step forward usually remains forgotten. The first two episodes of the series are dedicated to the truly exciting historical context of communication development, and some of the most important moments of the modern history of the Internet in the 1980's and 90's.

EPISODE 3 - "FREEDOM OF SPEECH"

The principle of the freedom of speech as a fundamental human right stretches historically all the way back to the first political structures in Europe, such as the Roman Empire. In the beginning slowly, and then gaining speed since Gutenberg's invention of printing press, the development of communication technology shapes the very comprehension of freedom of speech, affects social dynamics, undermines the boundaries between the public and the private - that in the age of the Internet intertwine in unexpected ways.

EPISODE 4 - "A PACKAGE"

What actually happens in a fraction of a second, the time needed for an intended emoticon to appear after we click to respond to someone's Facebook status? The package we chose for the fourth episode contains all the information required for an ordinary like on Facebook. Its journey from routers, servers and hosts, takes place at breathtaking speed while its route connects Novi Sad via Belgrade, to Frankfurt, Cornwall, New Jersey, all the way to the Forest City in the United States, where Facebooks servers are located. This journey is also the story of the complex architecture of the global network.

EPISODE 5 - "PRIVACY"

Entire new industries emerged on the foundations of the information revolution, whereby information is considered to be the "new oil", as experts usually say. This means that today, even the most trivial piece of private or public information has a specific value, while the services provided by Google or Facebook are a matter of ownership resembling those of oil fields. How the data economy emerged, what kind of values it creates, which tricks do corporations use in order to hoard information, how legal systems treat those issues, and how our privacy is affected those are the questions we discuss in the fifth episode.

EPISODE 6 "RESISTING THE SURVEILLANCE"

The risks to the privacy of citizens are growing and becoming more complex. However, there are new strategies to defend against the invasion: from contemporary Luddites, who completely reject the use of new technologies, to activists who create new digital tools for defense, advocating legislative changes and participating in the free exchange of knowledge in their communities. The principle of privacy underwent some drastic changes under the influence of new technologies that enable massive collection of personal data and virtually unlimited space for their storage. It is the responsibility of human society to rethink the boundaries of the private and the public, since civil liberties won in the analogue past do not cease to matter in the digital present. Digital literacy has become a new ideal of the internet generation Enlighteners.

EPISODE 7 "THE MEDIA"

With commercially available technologies, the Internet has allowed each individual to become their own media outlet and an active participant in the media environment, with equal chances to influence public opinion as editorial journalism which observes legal and ethical norms. Information flood represents a risk to accurate, important and timely news, while the democratization of access undermines the accountability for a publicly spoken word. The interests of the traditional media industry have been gravely affected by the break of the monopoly, not only in the production and distribution of content, but also in the selection of participants in the public discourse. On the other hand, the challenges citizens face shake the very foundations of rights and freedoms, such as free access to knowledge, pluralism, and quality of information available. Today one can no longer be even a passive media user without some knowledge of technological innovation and the mechanisms of access to content and services on the Internet.

EPISODE 8 "SECURITY"

Every day we hear about the numerous benefits but also the dangers of the cyber world. It is much easier to commit many crimes than it is the case in the "analogue" space fraud, theft, identity theft, and the like. However, new technologies have brought some specific infringement which we did not know of. Our identity, reputation, bank accounts are exposed, but also the entire municipal systems that have become digitized. In this episode we talk about Internet risks and how to protect our security. The experts will explain why it is important to have good passwords, what a two-stage verification means, and how to maintain "digital hygiene". We also talk of the cases that go beyond ordinary means of protection, when it is needed to turn to high-tech crime police units.

EPISODE 9 "AVATARS AND PERSONALITIES"

Every person on the planet is a unique individual. Even twins differ among themselves. Our identity is a unique mix of genetic and cultural heritage, everyday coincidences which determined the direction and course of our development, the decisions that we made freely or under pressure, and the decisions that were made for us. The Internet has enabled direct communication among people across the globe, leaving considerable room for them to adjust the parameters of their participation. This can sometimes seem like an opportunity to reinvent ourselves, and make a new or better version. In online games, for example, we can choose an avatar that is not of the same sex as our "real" person; on social networks we can create an entirely new character, protected by the feeling of assumed anonymity. In the ninth episode we talk about the psychological and social aspects of two identities, of cases in which the "avatar" won over their own personality, as well as the benefits and the risks of fluid identities of the digital age.

EPISODE 10 "THE INTERNET OF THINGS AND ARTIFICIAL INTELLIGENCE"

While the generations born before the digital revolution have an impression to already live the future described in the old SF novels, really radical changes are yet to follow. The development of artificial intelligence, the Internet of things, virtual reality, and other similar ideas is still in the early stages of transition from mere theory in wide use, but the knowledge and the necessary technology are already here. In the final episode, we talk about the technological development that has produced smartphones and smart refrigerators, creating an ever wider network of connected home appliances and utilities, which provides basis for smart cities. A new world emerges before our eyes, and although we are equally fascinated by various inventions – it is time to talk about the dangers appearing on the horizon.

8. SHARE FOUNDATION'S CONSULTING AND TRAINING

The SHARE Foundation offers a variety of consulting sessions and trainings on digital security and internet media law:

DIGITAL SECURITY FUNDAMENTALS

The focus of this basic level training is different aspects of Digital Security. First of all, it is important to note that not all risks are technological, but that the security of the system also depends on the user's habits.

ORGANIZATIONAL ASPECTS OF DIGITAL SECURITY

There is a set of measures, protocols and policies that can be implemented in an organization so that it can be digitally more secure. The hardware and software that are used on a daily basis are of vital importance. Finally, it is impossible to learn how to secure the system only through trainings, which is why it is important for users to know where to find good resources that will inform them more about Digital Security.

MANAGEMENT OF WHISTLEBLOWING PLATFORMS

This training is about the tech aspects of whistleblowing. The goal of the training is for the receivers of potential leaks to know how to protect their privacy, the privacy of the whistleblower, and how to manage a whistleblowing platform. In this way the role of tech personnel in the process of whistleblowing is minimized, which increases the reliability of the platform.

APPLIED DIGITAL SECURITY

This training is conceptualized as an addition to the aforementioned tech trainings. Essentially it consists of live demos of secure software. The goal of the training is to teach users how to practically implement secure protocols in the use of technology.

LEGAL RISKS IN ONLINE MEDIA

The training consists of making participants familiar with the current legal framework that applies to online media, depending on the type of media that is used for activism. The focus of this training is on the legal aspects of publishing and information sharing in the online environment and the right to privacy. One of the goals of this training is to introduce online media and digital activists to the legal fundamentals of the digital environment, while the ultimate goal is that participants learn about their rights and obligations and the responsibilities that can be associated with them in the legal system.

INTERNET PRIVACY ATLAS - THE INTERNET MAP OF SERBIA

The Internet in its essence is not what most people perceive when online. It is an abstract space which gives limitless opportunities, but it essentially consists of hardware, millions of servers, routers, cables, and other peripheral network devices. Basically, in most cases, there is a physical cable or wireless connection reaching almost every corner of the world and each internet user. Each and every network device of the Internet infrastructure has its own physical location. Some of them are grouped, which makes their locations a sort of "crossroads" of the Internet.

One of the reasons we seldom discuss the issues of this invisible infrastructure is the fact that content travels through the network so fast that that it is unnoticeable to us, in most cases we do not feel a significant difference between our packets are traveling just around the corner and around the world and back.