Abstract

Information and communication development brought new dangers for citizen’s rights and privacy. Information as a new power will largely determine the position of states and their administrations, and then the position of citizens and the private sector in the global game. In the last decade, the Republic of Croatia follows the trend of IT public sector, with less or more successes in certain segments. The field of my research work is the elaboration of issues of information security and protection of personal data and access to information through an overview of the current regulatory and legal data protection framework in the Republic of Croatia.

Presented at the Transatlantic Students’ Conference
Addressing Diplomatic, Economic, and Migration Challenges in Southeastern Europe
James Madison University
Florence, 23-27 April 2018
CONTENTS:

1. INTRODUCTION ..................................................................................................................... 2

2. CYBER SECURITY .................................................................................................................... 2
   2.1. THE CONCEPT OF CYBER SECURITY .................................................................................. 4
   2.2. PERSONAL DATA ON CYBERSPACE .................................................................................. 4
   2.3. REASONS FOR CYBER ATTACKS ...................................................................................... 6
   2.4. POSSIBILITY OF AN ATTACK ON A COMPUTER ................................................................. 6

3. PUBLIC ADMINISTRATION ..................................................................................................... 7
   3.1. E-GOVERNMENT .................................................................................................................. 8
      3.1.1. E-CROATIA .................................................................................................................. 9
      3.1.2. E-CITIZENS ................................................................................................................. 9
      3.1.3. E-COUNSELING ......................................................................................................... 11
      3.1.4. DATA.GOV.HR .......................................................................................................... 14

4. CYBER SECURITY AND PUBLIC ADMINISTRATION .............................................................. 15
   4.1. PUBLIC INFORMATION SPACE ......................................................................................... 16
   4.2. ISO 27001 .......................................................................................................................... 19
   4.3. ISO 27002 .......................................................................................................................... 20

5. SAFETY PROBLEMS ............................................................................................................... 21
   5.1. PROCEDURES IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION ............ 23

6. LEGAL FRAMEWORK IN REPUBLIC OF CROATIA AND PRACTICE ................................. 23
   6.1. CROATIAN LEGAL FRAMEWORK FOR PROVISION OF CYBER SECURITY ............ 25
   6.2. THE RIGHT TO ACCESS INFORMATION ......................................................................... 27
   6.3. NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF CROATIA ............................ 30
   6.4. INFORMATION SECURITY INSTITUTIONS IN THE REPUBLIC OF CROATIA ........... 31

7. HIGH-PERFORMANCE COMPUTING ...................................................................................... 36

8. CONCLUSION .......................................................................................................................... 37

9. REFERENCES ........................................................................................................................... 37
1. INTRODUCTION

The cyber world is something that changes on an everyday level and what needs to be adjusted because it’s spreads every level of society and the state. The development of the Internet also changes public administration. There is an increase in online public services. Does this increase threaten the fundamental human right to access information and human rights to the protection of personal data? In this paper, I will describe how Croatia applies new technologies and aligns them with legislation in relation to the protection of personal data.

In this paper, I present how important it is to ratify the Convention on Access to Official Documents as the first international document that systematically determines the right to access information. According to Information Commissioner Republic of Croatia, dr.sc. Anamarija Musa: "The fact that only 10 out of 47 Council of Europe States have ratified the Convention (as well as attempts to do the same by the EU directive or ordinance binding on member states) shows that there is resistance to the adoption of these highly-standardized standards. However, it should be noted that in Croatia the right to access to information guaranteed by the Constitution (Article 38/4) is regulated by the Law on Access to Information (Official Gazette 25/13, 85/15) which is one of the best in the world (www.rti-rating.org).

As an information commissioner I have sent an initiative to the Ministry of Administration to ratify the Convention and I hope this will happen. However, there is a danger that the current factual and legal compliance of our Right to Access to Information Act with the Convention will be interpreted as the absence of the need to ratify it. The adoption of the Convention would have greatly strengthened the legal framework for exercising the right of access to information, since in that case the Convention would have a higher legal force and prevented the limitation of that right."

2. CYBER SECURITY

The modern world carries a number of changes, the greatest technical advances, but also destructive wars, ecological disasters, technological catastrophes, and more and more difficult
economic crises. The work is an IT revolution, urbanization \(^1\) and globalization on the foundations of capitalism that deepens all of the social contradictions. The pace of progress in the area of information technology can’t be measured with the speed of progress in any other area. Such progress has made enormous increase in the availability of information so that all of the information available to us is difficult to find out the most important ones. Further development of high-tech information becomes more and more accessible, even with the farthest places. The IT revolution started with the emergence of an Internet package to connect devices around the world. The Internet carries a wide range of information resources and services, such as interconnected documents and applications World Wide Web\(^2\) (www), electronic mail (e-mail\(^3\)), telecommunications and file sharing.

The basic setting on which cyber society is based is the free exchange of information. Information has become a means of power and / or power since the earliest social organizations and order. At the end of the 20th century, in the era of general computerization (of course, only in technologically developed countries), "information" is of crucial importance. The conditions of modern technology, primarily computer technology. However, mobile communications, telephone communications and audio-visual communications can’t be ruled out. All this enters into the sphere of the so-called. Cyber society, whose action takes place in real time, but in an invisible, virtual space. A wide availability of technology enables increased automation of attacks and the use of sophisticated tools for attacking.

Such a consecutive and rapid rise of the Internet is accompanied by the same speed and the spread of misuse. By expanding and connecting, and especially by globalizing computer networks, new forms and methods of computer crime are emerging, and its effects become more and more dangerous, affecting the privacy of people, the whole branch of business, large businesses, and national and regional economies. Likewise, computer crime requires ever greater resources and better methods of protection against such abuses. However, in order to protect or

---

\(^1\) The world is undergoing the largest wave of urban growth in history. More than half of the world’s population now lives in towns and cities, and by 2030 this number will swell to about 5 billion, according to the research UNFPA (United Nations Population Fond)(https://www.unfpa.org/urbanization)

\(^2\) The World Wide Web (abbreviated WWW or the Web) is an information space where documents and other web resources are identified by Uniform Resource Locators (URLs), interlinked by hypertext links, and can be accessed via the Internet. (https://en.wikipedia.org/wiki/World_Wide_Web)

\(^3\) Electronic Mail (email or e-mail) is a method of exchanging messages ("mail") between people using electronic devices. Email first entered limited use in the 1960s and by the mid-1970s had taken the form now recognized as email. (https://en.wikipedia.org/wiki/Email)
at least minimize its adverse consequences, it is necessary to study its origin, development, characteristics, and appearing forms in which it occurs. Policy makers have a key role to play in ensuring that both public and private entities are well-equipped to face the challenges of cybersecurity in the increasingly connected world. They can do this not only by establishing appropriate legal and political frameworks, but by promoting awareness of cybersecurity security and collaboration with various actors involved in cyber-resilience.

A key component, and in many ways the foundation, of this framework is a national cybersecurity strategy, which is critical for managing national level cyber risks and developing appropriate legislation to support those efforts. A strong cybersecurity strategy should be a “living document,” developed and implemented in partnership with key public and private stakeholders. It should contain clearly articulated principles and priorities that reflect societal values, traditions and legal principles.

2.1. THE CONCEPT OF CYBER SECURITY

Cyber Security is a set of measures and procedures to secure data stored on computers, often accessible over the Internet, and covers data protection against loss or damage as well as unauthorized access to them. Nowadays, when most of the data is stored in computers, mostly and only in that form, and when much of the business, communication and the like takes place in a computer environment, loss or misuse of data can cause great damage.

The security of the information system is reflected in three segments (C-I-A) – Confidentiality (The data is confidential when it is incomprehensible to anyone except those authorized for its use)\(^4\) – Integrity (Data has integrity for as long as the identical state that was created after the last authorized user ended with it) – Availability (Data is available when they are available to authorized users in agreed format and reasonable time).

2.2. PERSONAL DATA ON CYBERSPACE

\(^4\) (ISO/IEC 27001: 2005)
Cyberspace⁵ is all the computer networks in the world and everything they connect and manage. It's not just the Internet. There is a difference. Cyberspace includes the Internet and various other computer networks that should not be available over the Internet. Cyberspace is actually quite ordinary. It's every laptop that people carry around, every desktop at work or at home, every USB stick, CD and tube down the street. In this cyberspace, personal data is stored and processed. Personal data must be processed fairly and legally. Under the Personal Data Protection Act ⁶ in the Republic of Croatia personal data may be collected and processed further:

- with the consent of the respondent only for the purpose for which the respondent has given the benefit, or
- in cases determined by law, or
- For the purpose of meeting the legal obligations of the head of the personal data collection, or
- for the purpose of concluding and executing the contract in which the respondent is a party, or
- for the purpose of protecting the life or bodily integrity of a respondent or other person in the event that the respondent is physically or legally unable to give his / her consent, or
- if the processing of data is necessary for the fulfillment of tasks carried out in the public interest or in carrying out the public powers held by the head of the personal data collection or third party to which the data are supplied, or
- If data processing is necessary for the purpose of legitimate interest of a data collector or a third party whose data is disclosed, unless the interests of the fundamental rights and freedoms of the respondents referred to in Article 1 paragraph 2 of the Personal Data Protection Act are prevailing, or
- If the respondent has disclosed this information.⁷

Personal data today are in the collections of personal information of the IT form. Personal data processing is any activity or set of actions made on personal data, whether automated or not, such as collecting, capturing, organizing, saving, modifying or modifying, retrieving, inspecting, using, disclosing, transmitting, posting, or otherwise available, categorized or combined, blocked, deleted or destroyed, and the implementation of logical, mathematical and other

---

⁵ The name was coined by American writer of science fiction William Gibson (1948), and became popular thanks to his novel Neuromancer (1984), which is the foundation of cyberpunk's direction in scientific-literary literature. (source: http://www.enciklopedija.hr) For the cyberspace, Gibson has said that this is an "agreed hallucination every day experienced by millions of legitimate operators of all nations", i.e. "graphic presentation of data extracted from the warehouse of each computer integrated into the human system.

⁶ Official Gazette 103/03., 118/06., 41/08., 130/11., 106/12

⁷ Article 7. Official Gazette 103/03, 118/06, 41/08, 130/11, 106/12
operation with these data. The provisions of the Personal Data Protection Act apply to the processing of personal data by state bodies, local and regional self-government bodies, as well as legal and natural persons, representations and affiliates of foreign legal entities and representatives of foreign legal and natural persons.

2.3. REASONS FOR CYBER ATTACKS

The reasons for cyberattacks are the realization of unlawful benefits and for deliberate and conscientious damage. The resulting damages can be tangible, intangible, business, political, national and personal. Information is a resource and has become crucial in today's world of high technology. One who has the right information at the right time has power and therefore attaches great importance to today's information and information systems.

The World Economic Forum cyber attacks has ranked third in the rankings of the greatest risk for humanity in the future. Thus, cyber attacks have been declared the third most dangerous act that can greatly harm humanity and humanity globally. In front of the cyber attack on the ladder of danger, only natural disasters and extreme weather conditions were found. So these are the three most dangerous things that threaten mankind, of which two are caused by the very nature we can not influence, while this third is caused by man.

2.4. POSSIBILITY OF AN ATTACK ON A COMPUTER

The possibilities of unauthorized intrusion into the computer are very likely. Unfortunately, unidentified guests or intruders are extremely inventive when it comes to entering the computer.

Four types of security incidents:

1. Natural Disaster - In the last few years, the world has experienced several natural disasters, such as hurricanes Katrina and Sandy, disaster Fukushima, tsunami and earthquake

---

8 https://www.weforum.org/agenda/2017/01/these-are-the-most-likely-global-risks-2017/
9 one of the five deadliest hurricanes in the history of the United States, at 2005.
10 it was the second-costliest hurricane on record in the United States until surpassed by hurricanes Harvey and Maria in 2017.
11 was an energy accident at the Fukushima Daiichi Nuclear Power Plant in Ōkuma, Fukushima Prefecture, initiated primarily by the tsunami on 11 March 2011.
like the one in Haiti\textsuperscript{12}, destroyed entire companies and data banks. Even a localized fire may destroy all data.

2. \textit{Malicious attack (external source)} - is done by unauthorized remote access from any other location, usually via telephone connections. For this purpose, the so-called "social engineering"\textsuperscript{13}. Access can also be achieved by using an automated tool, a software solution for finding the appropriate password. As for the attacker, this is mostly the so-called hackers\textsuperscript{14}. The motives of such attackers can move from the most disadvantaged to far more dangerous.

3. \textit{Internal attack} - Unauthorized access and loss of data may come within the information system itself, by persons who can physically access them (such as employees, service providers, suppliers, etc.). One of the most famous cases in recent years is the one who shook the CIA and the NSA (National Security Agency), Edward Snowden, a former NSA employee, which in 2013 released top quality documents over the Guardian and the Washington Post, regarding various NSA programs, including mass monitoring programs PRISM \textsuperscript{15} and xkeyscore\textsuperscript{16}.

4. \textit{Malfunction and unintentional human error} - Equipment failure and infrastructure are something we encounter almost daily - loss of power, failure of internet connections and phone lines, slamming of hard disks, but also accidentally shaded coffee cup over the computer, or faulty data. Such incidents happen very often.

\section{3. \textsc{Public Administration}}

\textsuperscript{12} was a catastrophic magnitude 7.0 Mw earthquake, with an epicenter near the town of Léogâne on Tuesday, 12 January 2010.

\textsuperscript{13} Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access. (https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)) The best known: Shoulder surfing

\textsuperscript{14} Hacker is any skilled computer expert that uses their technical knowledge to overcome a problem. While "hacker" can refer to any skilled computer programmer, the term has become associated in popular culture with a "security hacker", someone who, with their technical knowledge, uses bugs or exploits to break into computer systems. (https://en.wikipedia.org/wiki/Hacker)

\textsuperscript{15} PRISM is a code name for a program under which the United States National Security Agency (NSA) collects internet communications from various U.S. internet companies.

\textsuperscript{16} XKeyscore or XKEYSCORE (abbreviated as XKS) is a formerly secret computer system first used by the United States National Security Agency for searching and analyzing global Internet data, which it collects on a daily basis.
The governments of the future will have to adapt to the growing of Internet infrastructure and are constantly evolving to create the values needed for their citizens. They need to remain ready to respond to the current changes and to build capacity for effective public administration. What we need today is called the FAST government, it is smoother, more agile, modern and technologically equipped.

Government in 21st century will mark the decline in the size of the civil service in many countries. Some public administration jobs will disappear, some will go completely to the private sector. Machines will in many ways replace human resources, which will have to change the public administration and make new adjustments. Also, we are aware of the increasing involvement of citizens in the decisions of local and regional public administration. People want to express their attitude, opinion, want to be involved in issues that directly affect their lives.

The problems which facing the 21st government and the public service, are the concepts of open government and open data. There is a public discourse about what public information is. But on the other hand, the same government uses data and power that are available on the Internet, on social networks, on various mobile applications, to manipulate the will of citizens. The public administration itself will not be able to develop enough capacity to provide basic services to citizens. Yet, the market alone will not have the power to be able to generate public value independently. For this reason, the public administration must develop to the fullest extent. The power of the state will be counted on the strength of adapting public administration to new times. Although great differences will remain between governments, there are established world standards, best practices and lessons learned that will be set as a standard of management. The governments of the future will need to adapt and develop continuously to create the required and required social values. They have to change quickly according to the expectations of citizens. Citizens demand a more transparent state leadership, a more honest division of public funds, a responsible public administration.

The balance between risk management and open hair is the answer to the key political and business issue faced by public officials in terms of how best to implement an open government, open data and social media in the government.

3.1. E-GOVERNMENT
E-Government is the use of electronic communication devices, computers and the Internet to provide public services to citizens and other persons. It represents the interaction of deliveries of state products and services, information exchange, communications and transactions. E-government contributes to the functioning of democracy through online provision of government information. It is the second revolution in public management, which may transform not only the way in which most public services are delivered, but also the fundamental relationship between government and citizen.

There is a difference between government and government (G2C) government and business / trade (G2B) between Government and other government agencies (G2G) between government and business (G2C) between government and business / commerce (G2B) between citizens and their government (C2G).

3.1.1. E-CROATIA

The Government of the Republic of Croatia has adopted on several occasions various strategies related to the computerization of state administration. Thus, we have the Strategy for the Development of Electronic Business in the Republic of Croatia for the period 2007-2010, the Operational Plan for Implementation of the e-Croatia 2007 Program and the Croatian Framework for Interoperability (HROI) from 2010, which should improve the work of the state administration with the aim of making citizens more accessible and transparent. Some of the services that have survived are: e-Health, e-Regos, e-Taxes, e-Citizens, e-books, e-Charter\textsuperscript{17}, e-Invoice.

According data \textit{International Telecommunication Union (ITU), World Bank, and United Nations Population Division} in 2016. Croatia internet users was 3 133 485, which is 74,2% of population\textsuperscript{18} and sets Croatia on 91rd World Position Rankings\textsuperscript{19}.

3.1.2. E-CITIZENS

\textsuperscript{17}The only thing that is entirely done electronically is the one that has applied the advanced electronic signature
\textsuperscript{18}http://www.internetlivestats.com/internet-users/croatia/
\textsuperscript{19}http://www.internetlivestats.com/internet-users-by-country/
The e-Citizens system is a project of the Government of the Republic of Croatia with the aim of modernizing, simplifying and accelerating the communication of citizens and public administration and increasing public sector transparency in providing public services. This project provides access to public information and public service information in one place, secure access to personal voices and electronic communications between citizens and the public sector.

The e-Citizen project will be implemented through three main components, which will make the public sector's common infrastructure:

- System of the central state portal - whose management is in charge of the Office of the Prime Minister of the Republic of Croatia.
- National Identification and Authentication System (NIAS) - whose management is in charge of the Ministry of Administration.
- Personal User Box System (OKP) - whose management is in charge of the Ministry of Administration.

However, where appropriate, projects may include other stakeholders with whom appropriate contracts or agreements will be concluded. These participants can come from the private sector, as well as the key to public private partnerships.

The Central State Portal is a project that brings together the Government of the Republic of Croatia in one place and in easily accessible forms of information on public services as well as information and documents related to the implementation of the policy.

Each component solves part of the issues mentioned. The central portal addresses the issue of dispersion of information and e-services, the National Identification and Authentication System - NIAS addresses the issue of electronic identity verification and has developed a network for issuing one type of access element, and the Personal User Box (OKP) represents a mechanism for secure delivery of personalized information to users. The Ministry of the Interior has issued an electronic identity card (eOI) with an identity certificate, which is also the highest level credential, allowing access to all electronic services. Within the framework of e-Citizens' establishment, the Republic of Croatia has also provided the Contact Center e-Citizens as the central point of contact and support for all current and potential users of e-Citizens. The purpose of establishing the Central Contact Center e-Citizens is to provide adequate and fast customer

---

20 Official Gazette 53/13
support in the part of the use of electronic services as well as providing informative support to the work and capabilities of the system\textsuperscript{21}.

Almost all public sector bodies have developed e-services, and citizens of the Republic of Croatia from 10 June 2014 have been able to use the internet service e-Citizens\textsuperscript{22}.

The number of e-Citizen users who have been authenticated at least once through NIAS on one of the e-services since 10 June 2014. is the highest in the City of Zagreb, with 7,054 registered on day 30. June 2014. increased up to 71,880 registered on day 31. December 2015. According to the number of users, and at the very end of the Lika-Senj County with 111 registered corridors on 10 June 2014, up to 1,273 users registered on 31 December 2015\textsuperscript{23}.

<table>
<thead>
<tr>
<th>County Name</th>
<th>Number of unique users \textsuperscript{1}</th>
<th>Share (%)\textsuperscript{2}</th>
</tr>
</thead>
<tbody>
<tr>
<td>City of Zagreb</td>
<td>164,373</td>
<td>31,17%</td>
</tr>
<tr>
<td>Split-Dalmatia County</td>
<td>42,123</td>
<td>7,99%</td>
</tr>
<tr>
<td>Primorje-Gorski Kotar County</td>
<td>42,107</td>
<td>7,99%</td>
</tr>
<tr>
<td>Lika-Senj County</td>
<td>3,435</td>
<td>0,65%</td>
</tr>
<tr>
<td><strong>TOTAL in Croatia</strong></td>
<td><strong>527,283</strong></td>
<td><strong>100,00%</strong></td>
</tr>
</tbody>
</table>

\textsuperscript{1} Number of unique users - number of e-Citizens who have at least once identified through NIAS on one of the e-services, where the county is determined by the place of residence of the user.

\textsuperscript{2} Share (%) - the ratio of the number of users in each county compared to the total number of users.

Picture 1. *Statistical report from the National Identification and Authentication System (NIAS) dated 01.06.2014. to 01.03.2018., source: https://data.gov.hr/dataset/e-gradjani-statistika*

Forecasts are that 75\% of citizens of the Republic of Croatia will use e-services through the e-Citizens system by 2020.\textsuperscript{24}

3.1.3. E-COUNSELING

The Government of the Republic of Croatia is in its program for the mandate period 2011-2015. sets two important goals, namely to create open and transparent public

\textsuperscript{21} e-Croatia 2020 Strategy
\textsuperscript{22} http://www.aaiedu.hr/o-sustavu/povezani-sustavi/e-gradani
\textsuperscript{23} Statistical report 24.02.2016.g., Ministry of Administration. Number 1
\textsuperscript{24} e-Croatia 2020 Strategy, Indicators on the use of public administration services through the Internet for citizens
administration and increase access and service to citizens by using information systems. Portal of e-Consultancy was launched on April 27, 2015.25

The Portal of e-Counseling enables the participation of users in the consultation process with the interested public, which enables the unification of all open consultations at one place, a quick and easy search for open consultations and effective advocacy of all interested social groups and individuals in the policy-making process in accordance with the Act on Impact Assessment regulations. The Office for Associations is responsible for coordinating the establishment and use of e-counseling portal. All state administration bodies should conduct public consultations through the Central Internet portal for e-counseling, as this obligation is expressly provided for in Article 11, paragraph 2 of the Act on Access to Information Act26. Advising through the portal e-Counseling does not exclude the obligation of the public authorities to inform the public about public consultation as a procedure and about ongoing consultations on their web pages.27

The standardization of the consultation process with the interested public in the Republic of Croatia started with the adoption of the Code of Conduct for interested public in the procedures for the adoption of laws, other regulations and acts at the session of the Government in November 200928. Accordance with the Code, all state administration bodies were required to appoint advisory coordinators, and the Office for Associations should have developed guidelines for the implementation of the Codex and a systematic training program for the Coordinator for Counseling. During 2010, the Guidelines were developed and the first co-ordinators were also trained, and in accordance with the Code several consultations with the interested public were conducted.

According to the data available to the Governmental Office of the Government of the Republic of Croatia in 2016, a total of 642 consultations with the interested public were conducted in the procedures for the adoption of laws, other regulations and acts. This is 6% more than in 2015 when 608 consultations were conducted. Compared to 2014, when 544 public consultations were conducted, this is an increase of 18%, compared with the year 2012 when the state bodies carried out 144 consultations, in 2016, an increase of 445%.

26 Official Gazette 25/13, 85/15
27 Publication of information on public consultations on the website of the state administration bodies, Analytical Report on Monitoring the Implementation of the Act on the Right to Access Information, Number 3/2017
28 Official Gazette 140/09

In the year 2016 there were 12,856 comments on drafts of laws, other regulations and acts. Graph 2 shows percentages of accepted, unaccepted, partially accepted, received, and non-responsive.


It is currently in the process of e-counseling and the new Bill of Laws on the Implementation of the General Data Protection Act, which provides for the implementation of
EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement such data. This law should come into force in May this year (2018). By the day of writing this work, on the portal e-Counseling, a total of 267 comments were submitted to the articles of the Proposal, 215 general comments and 52 text updates. The majority of the comments refer to Art. Article 45, paragraph 1, which reads: "A violation of this Law or the General Regulation on the Protection of Data may not be subject to an Administrative Penalty to the authority of the public authority." The largest number of comments relates to unfairness and discrimination between public and private entities the authorities of the public authorities are expelled and all the others are placed in an unequal position. It also points out that such an article affects the protection of the personal genius of citizens whose personal information is being processed by the public authorities. It is necessary to equally prescribe the obligation to apply administrative fines to all taxpayers in the same way.29

3.1.4. DATA.GOV.HR

The Open Data Portal of the Republic of Croatia is a data node that serves to collect, categorize and distribute open data from the public sector. In accordance with the Global Open Government Partnership initiative30, The Portal represents a data node that serves to collect, categorize and distribute open public sector data and is a kind of continuation of the policy of transparency and openness of the work of the public authorities.

The goal is to improve the spread of public and open data across a single and central site and to enable the creation of innovative non-commercial and commercial applications that would use this data. It also intends to encourage more intensive cooperation with the private sector.

29 https://esavjetovanja.gov.hr/ECon/MainScreen?entityId=6988
30 Open Government Partnership is a multilateral initiative aimed at ensuring concrete progress in the area of transparency and openness of the work of the public authorities, the involvement and empowerment of citizens and civil society, the fight against corruption and the use of new technologies to improve the quality of services provided by public administration to citizens. The initiative is chaired by the Steering Board, whose members are representatives of governments and civil society organizations. From 2014, the member of the Steering Board is also the Republic of Croatia. The initiator of the Initiative is US President Barack Obama, who in his speech at the UN General Assembly in September 2010 announced the basic principles, largely based on the Open Government Directive, one of the cornerstones of his program. (https://udruge.gov.hr/partnerstvo-za-otvorenu-vlast-271/271)
The Open Data Portal is run by the Central State Office for the Development of a Digital Society with the technical support of the Ministry of Administration, and the Digital Information Documentation Office, which provides access to public official documents (international agreements, legal regulations, documents and publications of public authorities) and information of the Republic of Croatia.

Public authorities shall, whenever possible and appropriate, publish readily available information (open data) together with metadata, in a computer readable and open form, in an easily searchable manner. In addition, through data.gov.hr, citizens may file a request for reuse of data, and the Appeals Commissioner is responsible for appeals against such requests.

According to Open Data European Portal Croatia is on the right track and is in the group of leaders in the Open Data field. But it also states that there are more obstacles to even better and more effective data openness. Among them, they cite political barriers, where stronger coordination between the public sector bodies is needed. Then a technical barrier in which more frequent data updating is required. Legal barrier, some data sets charge above the marginal costs. Inadequate access, where work is needed on public sector bodies to raise awareness of open data and organize workshops to train civil servants to publish data.

**Graph 3.** *Open Dan in Croatia during 2016. and 2017., Source: European Data Portal, Made by: Petra Baničević*

4. **CYBERY SECURITY AND PUBLIC ADMINISTRATION**
Internet development also changes public administration. There is an emergence of online public services and this is a key development factor in which public administration is changing. In this way, public administration quickly supplies access to public services, both to citizens and businesses. However, by adopting new technologies in public administration, they also exposed them to a new kind of threat, so-called cyber threats.

So today it is no longer just enough to look after typical IT problems, such as preventing or reporting incidents. Many public authorities have implemented new technologies without paying attention to the risk-taking requirement and will now have to make additional efforts to adapt to the new legal landscape. Cyber threats represent a constant and significant security risk for the public administration. So great a threat to become a powerful weapon to attack the citizens and the public agencies of the countries. Such threats can seriously affect the quality of services and, more importantly, steal confidential information, from private data to state secrets.

In order to prevent attacks on public bodies, a common regulatory and legislative framework is needed with responsibilities between the states. One such example is the new regulatory framework adopted in the EU in 2016\(^\text{31}\). With regard to the existing legal framework, the Regulation significantly unifies the handling of personal data processing at the level of the European Union.

\section*{4.1. PUBLIC INFORMATION SPACE}

The information space represents a virtually global environment of interrelated public and private information systems, where different types of data are generated and transmitted, as well as different types of specific data. Consequently, it is necessary to apply the information security measures and standards prescribed for the protection of confidentiality, availability and comprehensiveness of data and the availability and completeness of the information systems in which such data are processed, stored or transmitted.

There are several phases through which the design of the public information space has passed. At the very beginning of the information space, there is a strong boundary between the

\footnote{31 The new European regulatory framework for the protection of personal data, such as the Universal Data Protection Regulation 2016/679 and Directive 2016/680 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, investigation, detection or prosecution of criminal offenses or execution criminal sanctions and free movement of such data was adopted in mid-2016 and will apply in all EU Member States on 25 May 2018}
public and the secret. This sharp boundary at that time was further underlined by the discretion of deciding the state bodies on the boundaries between the public and the secret part of the information space. The secret space belonged entirely to the state sector in the narrow sense, mostly for the security, intelligence, police and military sectors, and the data were almost completely closed to the general public.

As the policy shifted globally, and as the battlefield itself went into the field of state administration, the need for international co-operation and the formation of international standards of security information security models emerged. This distinguishes classified, unclassified personal data, and security models for the implementation of security policy goals. Some of the models like the Bell-LaPadula model\(^{32}\) and Lattice Model\(^{33}\), which elaborate data access control on the information system, focusing on the security criterion of confidentiality of such data, or the Biba model \(^{34}\) which focuses on the data integrity criterion as well as a whole host of other formal security models.

An integral part of the information system is its environment, which along with the technical system includes system information and system users themselves. In order to know who, when and under which conditions it has access to certain levels of information, it is necessary to develop the security system information system. Thus, the security mode of information systems is linked:

---

32 The Bell-LaPadula Confidentiality Model is a state machine–based multilevel security policy. The model was originally designed for military applications. State machine models define states with current permissions and current instances of subjects accessing the objects. The security of the system is satisfied by the fact that the system transitions from one secure state to the other with no failures. The model uses a layered classification scheme for subjects and a layered categorization scheme for objects. The classification level of the objects and the access rights of the subjects determine which subject will have authorized access to which object. This layered structure forms a lattice for manipulating access. The Bell-LaPadula Confidentiality Model is a static model, which assumes static states. It implements mandatory access control (MAC) and discretionary access control (DAC)... (https://link.springer.com/referenceworkentry/10.1007/978-1-4419-5906-5_773)

33 Lattice-based access control models were developed in the early 1970s to deal with the confidentiality of military information. In the late 1970s and early 1980s, researchers applied these models to certain integrity concerns. Later, application of the models to the Chinese Wall policy, a confidentiality policy unique to the commercial sector, was demonstrated. A balanced perspective on lattice-based access control models is provided. (http://ieeexplore.ieee.org/abstract/document/241422/?reload=true)

34 The Biba Integrity Model is a hierarchical security model designed to protect system assets (or objects) from unauthorized modification; which is to say it is designed to protect system integrity. In this model, subjects and objects are associated with ordinal integrity levels where subjects can modify objects only at a level equal to or below its own integrity level. Model Biba Integrity Model is named after its inventor, Kenneth J. Biba, who created the model in the late 1970s to supplement the Bell–LaPadula security model, which could not ensure “complete” information assurance on its own because it did not protect system integrity. The Biba policy is now implemented alongside Bell–LaPadula on high assurance... (https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_774)
1. The degree of confidentiality of classified information on an information system
2. Level of security certificates of persons accessing the information system
3. The necessity of accessing classified information within the scope of a person's work
4. Formal Approval for Access to Information System Information

These elements from the safety starting point represent the basic elements for deciding on granting access to the system. Information within the information system varies depending on the availability levels. That's how we differentiate: dedicated, system high, compartmented and multilevel.

Persons in the state administration who access classified information will receive Certificates of appropriate degree of confidentiality in accordance with the degree of confidentiality of the confidential information they need for access. The security check process is initiated by the state body, for its employee who has the need to know (needs-to-know) within certain categories of classified information within the scope of his or her workplace.

In this way, clear and transparent regulations regarding the classification of data at interstate levels are brought about, leading to the obvious international exchange of classified information and the cooperation of various countries in areas such as military co-operation or the fight against modern skies, such as terrorism. The foundations of mutual trust between states are built on the basis of clear principles of classification and data protection and the application of appropriate, mutually agreed security policies.


35 Official Gazette, International Agreement 9/06
36 Official Gazette, International Agreement 5/09
37 Official Gazette, International Agreement 2/17
The security policy of the eighties of the last century further encouraged the closure of data at the national border. However, the rapid growth of information and communication technology and the rapid expansion of the Internet in the 1990s and later led to an ever-increasing link between the national IT space of different countries in a common global information space. Because of the strong expansion and global expansion and openness, there has been a new problem facing man in the 21st century, which is the protection of personal data. Not only does a man as an individual face personal data protection but institutions such as state bodies and other real people face the same problem.

At the level of governments and organizations, such as NATO or the EU, the protection of confidential data is labeled as Unclassified or Limited. Data marked Unclassified are an option that can prevent public insight into situations where such insight makes it difficult for further activities to address the content of unclassified data. Unclassified data characterized sensitivity in the sense of business or service relations, where such data is not classified as secretive and can’t be classified as a degree of secrecy. The most notorious example of the label Unrated in the state administration is the planning and preparation of future legal acts. Unclassified represent labels for non-confidential data, but are intended only for the official treatment of particular persons and are not permitted to be disclosed. The introduction of this level of data quality significance has led to a reduction in the number of classified data, resulting in greater transparency of the work of the state administration.

4.2. ISO 27001

ISO 27001 means for information security the same as ISO 9001 for quality - this is the norm written by the world's top IT specialists and its purpose is to provide a methodology for how to bring information security to an organization. It also provides the organization with a certificate, which means that an independent auditor has confirmed that information security is best implemented in the organization concerned. The ISO 27001 standard is in fact the foundation for information security, so different regulations are written based on the same - Decisions on Appropriate Information Management System, the Regulation on Storage and Special Measures of Technical Protection of Special Categories of Personal Data as well as

38 A. Klaić, A. Perešin – Concept of regulatory security information framework, 2011.g.
implementing acts of the Information Security Act. In other words, this standard provides an ideal methodology of how to implement all of these regulations.

"Norms are publicly available specifications that provide information security in the domain of information security to address certain aspects of information security."\(^{39}\)

Once security requirements have been identified and a risk assessment is made, appropriate controls have to be chosen and implemented to keep the risk at an acceptable level. The choice of control depends on the organization, and the acceptability of the risk and the manner of risk management, but also on the national and international legal rights and obligations.

The standards that are of utmost importance for the security of information systems are: ISO 27001 - Information Security Management System and ISO 27002 - Code of Information Security Management Procedures. In order to establish a quality system and information security management, it is necessary to use both standards.

In addition to the main standards, there are many others related to information security and security issues that have already been or are planned in the coming period:

ISO 27003 – SMS Implementation Guide
ISO 27004 – Measurement and metrics of the efficiency of the information security system
ISO 27005 – Information security risk management
ISO 27006 – Requirements for the process of analysis and certification of stand
ISO 27007 – ISMS Analysis Guidelines
ISO 27011 – Guidelines for the establishment of ISMS in the telecommunications sector
ISO 27031 – Specifications for the ICT Department of Preparedness for Continuous Business Continuity
ISO 27032 – Instructions for cyber security
ISO 27033 – Network security instructions

4.3. ISO 27002

ISO 27002 is an international standard that sets guidelines and general principles for launching, implementing, maintaining, and improving the organization's information security management. The goals outlined in this standard provide a general guideline for achieving commonly accepted goals in information security management. The objectives of control and control of this standard are intended to be applications that will meet the requirements arising from risk assessment. Implementation Steps:

1. The administrative phase - management or management makes a strategic decision to start the project. If security policy is not already in place, it is necessary to establish it.

2. Defining ISMS - Defining the scope of information security management, the scope may be the whole organization or just some of its parts.


4. Risk Management - Risk assessment results are compared with an acceptable level of risk and certain measures are taken to reduce the excessive risk to an acceptable level.

5. Training and Staffing - Signs a contract with all employees stating that they are familiar with the responsibility they have with regard to safety. It is necessary to ensure that all employees with a certain responsibility in the ISMS have the appropriate qualifications to perform their tasks.

6. Preparation for audit - it is necessary to make a Statement of Applicability before the audit itself.

7. Audit - may be the audit of documentation, implementation and third party.

8. Periodic Checks - Whether we have successfully passed the certification procedure or not, it is important to regularly review and improve the security management system. Inspections and system updates are very important because the security area is very variable.

5. SAFETY PROBLEMS

There is a wide array of activities that are considered to be cyber incidents: unauthorized data access or illegal exchange of data and software code, unauthorized or illegal use of applications, software piracy, viruses, compromising computer devices (DDoS attacks), physical destruction of computer and communication devices, etc. The security program must foresee and document the procedures and measures that will achieve a satisfactory degree of protection of
information resources and determine the rights and duties of system users and other persons who are in any relationship with those resources. Database security is a big problem for every institution and company, and so on state bodies. Any bigger job, such as health care or state institutions, relies on databases where they store key data. That's why it's very important to protect and manage the database in the right way. The security program consists of four components that need to be provided, relating to physical, human, communicative and operational security.

Physical Security includes all actions and measures aimed at preventing unauthorized access and endangering the computer system, other equipment, and the environment in which they are located, threatening them with events, things, and people. Various security measures such as physical security, alarm, surveillance, identification and fire protection systems and various biometric methods are used for this purpose.

Human Security covers all those actions and measures aimed at preventing harm that may arise through deliberate or accidental procedures of employees and other persons who have access to the system as well as other persons who are potential perpetrators of misuse. The threat to the system of an individual is greater than his rights to access to the system are greater, the greater the level of his expertise, and has a connection with his work motivation.

Communication Security includes measures aimed at securing secure, undisturbed, complete and secret communication and data exchange between authorized users by remote access or through various networks.

Operational security is primarily related to the protection of hardware and software, and is aimed at preserving their functional integrity. It also includes measures for damages from attacks on procedures used to prevent and detect misuse.

SOA\(^{40}\) has acted to detect and suppress state-sponsored cyberattacks. In 2016 the Agency identified at least 7 state-sponsored cyberattacks on the protected information and communication systems of the state bodies of the Republic of Croatia.\(^{41}\)

The main recommendations for maintaining database security are constant upgrading of software packages, separating the database on secure network segments, using encryption for transferring and storing sensitive data, using authorization for Identification, authentication, and

\(^{40}\) Security-Intelligence Agency
authorization. Although the databases are vulnerable to the mentioned external and internal threats, it is possible to reduce the vulnerability to an acceptable level of risk. This is achieved by using advanced security mechanisms, constantly upgrading operating system software packages, using secure network resources, and security products such as firewalls and antivirus tools.

5.1. PROCEDURES IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION

User Identification is a process by which a system requests a user to present in some way before entering the system. The security of data from unauthorized access and use (data protection) is achieved by authentication. This is a check of whether the user is really the person he represents. It is implemented by encryption, which implies the translation of information into a coded form that is only understandable to those who have the key to decoding it. It can be accomplished in two ways: as physical identification / authentication or as logical identification / authentication.

In computer networks, the user proves their identity with a password\textsuperscript{42}, PIN, a one-time password received by a token, a magnetic card, a smart card or a chip, scanning a fingerprint or iris (biometrics). However, it is considered that the identity of a person can be most safely determined by the determination of its characteristic bodily characteristics, for example by scanning a fingerprint or iris, and by other methods that are collectively referred to as biometrics.

6. LEGAL FRAMEWORK IN REPUBLIC OF CROATIA AND PRACTICE

The normative regulation of personal data protection in the Republic of Croatia is defined by the Personal Data Protection Act\textsuperscript{43} regulating the protection of personal data for natural

\textsuperscript{42} In order to protect it safely and securely, it is necessary to use a multiple combination of passwords (letters and numbers). For example, a 5-letter password consisting of lower-case letters is roughly approximately the same 8 x 10 \(^6\) (eight times ten to the power six) possible combinations, while the passphrase is composed of capital letters and ten digits have 776 x 10 \(^6\) (seven hundred seventy-six times ten to the power six) possible combinations. A user who creates almost all the characters for creating a password can create a 43 000 000 000 000 000 password. (Computer security, prof. dr. sc. Miroslav Bača, foj (https://www.scribd.com/document/59877924/FPZ-RS-PART-1).

\textsuperscript{43} Official Gazette 103/03., 118/06., 41/08., 130/11., 106/12.
persons and supervision of the operation of the personal data processing system in the Republic of Croatia. Personal data protection in the Republic of Croatia is secured to every natural person irrespective of nationality and residence, regardless of race, color, sex, language, religion, political or other belief, national or social origin, property, birth, education, social status or other features. The purpose of personal data protection is the protection of private life and other human rights and fundamental freedoms in the collection, processing and use of personal data. The Republic of Croatia has accepted the provisions of Convention 108 (Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data), as adopted by the Council of Europe, and the Croatian Parliament passed the Law on Confirmation of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data on 14 April 2005 Of the Additional Protocols to the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data with regard to Supervisory Authorities and International Data Exchange. Convention on Cybercrime has introduced the term “cybercrime” in the daily language of the legal profession, which has taken huge steps in the co-operation of signatory states in combating cybercrime, while the National Strategy for Cyber Security and the corresponding action plan define and describe areas of information technology that need to be protected.

Personal data processing is defined as any procedure or series of procedures that are performed on personal data - with or without automatic processing (AOP). These are: collection, recording, editing, storage, personalization or modification, retrieval, search, use, publication by transmission, dissemination, or otherwise by making available, classified or combined, blocked, deleted or destroyed data.

The European Union’s security standards, which require the introduction of all Member States, include requirements for the area of information security and the definition of national security policy in this area.

Harmonization of the existing national practice in the Republic of Croatia with EU security guidelines has led to the adoption of a series of laws and the establishment of a platform for the implementation of prescribed measures and standards of information security in all state bodies, local and regional self-government units, public authorities and other to legal entities that use classified and unclassified data within their scope.
Information security requirements are primarily due to the protection of the work of state bodies, notably because of classification and non-classification data, but it should be seen more widely than information security in the work of the state administration because the information security itself, because of the wider information space, has also been transferred to the modern society in the whole, which now becomes an information society and as such should protect it.

6.1. CROATIAN LEGAL FRAMEWORK FOR PROVISION OF CYBER SECURITY

Legislative regulations encompass a wide range of international and national legal regulations that in some way regulate information security in the Republic of Croatia. Since the independence of the Republic of Croatia in some services, a high level of data secrecy has been achieved. The concept of information security in Croatian practice was introduced several years before the adoption of the Security Services Act, within the framework of the Partnership for Peace program requirements (PfP) and cooperation with NATO. There are a number of laws, strategies, programs, action plans, rules and regulations that directly or indirectly address the issue of information / cyber security and critical (information) infrastructure.

Table 1. The chronological presentation of the various forms of legislative legislation in the Republic of Croatia, was made by Petra Baničević

<table>
<thead>
<tr>
<th>YEARS</th>
<th>IMPLEMENTATION FRAMEWORK</th>
<th>LEGISLATIVE FRAMEWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INTERNAL ACTS, REGULATIONS RULES, LAWS</td>
<td>RULES OF INFORMATION SYSTEMS SECURITY AND NATIONAL CERT</td>
</tr>
<tr>
<td>2002.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2003.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

44 Official Gazette 32/02
45 The Republic of Croatia joined the Partnership for Peace program on 25.05.2000 and the program left on 1.4.2009
46 North Atlantic Treaty Organisation
<table>
<thead>
<tr>
<th>Year</th>
<th>Legislation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2004</td>
<td>Regulation on the manner of storage and special measures for the technical</td>
<td>protection of special categories of personal data</td>
</tr>
<tr>
<td></td>
<td>protection of special categories of personal data</td>
<td></td>
</tr>
<tr>
<td>2005</td>
<td>The Electronic Correction Act</td>
<td>National Information Security Program in the Republic of Croatia</td>
</tr>
<tr>
<td>2006</td>
<td>Law on the Security and Intelligence System of the Republic of Croatia</td>
<td></td>
</tr>
<tr>
<td>2007</td>
<td>The Privacy Act, the Information Security Act</td>
<td></td>
</tr>
<tr>
<td>2008</td>
<td>Rulebook on the Privacy of Data Protection, MOHR(^47)</td>
<td>Ordinance on the layout, content and right of use of official identity card and official badge of official persons of the Institute for Security of Information Systems</td>
</tr>
<tr>
<td>2013</td>
<td>Rulebook on the manner and timelines for the implementation of security and integrity measures for networks and services</td>
<td>Rulebook on the manner and timelines for the implementation of security and integrity measures for networks and services</td>
</tr>
<tr>
<td></td>
<td>Rulebook on Methodology for Creating Critical Infrastructure Risk Analysis</td>
<td>Rulebook on Methodology for Creating Critical Infrastructure Risk Analysis</td>
</tr>
<tr>
<td>2014</td>
<td>Law on State Information Infrastructure, Regulation on the Establishment of a Public Register for the Coordination of State Information Infrastructure Design Projects</td>
<td>Law on State Information Infrastructure, Regulation on the Establishment of a Public Register for the Coordination of State Information Infrastructure Design Projects</td>
</tr>
<tr>
<td>2015</td>
<td>Ordinance on Amendments to the Ordinance on the manner and timelines for the implementation of security and integrity measures for networks and services</td>
<td>Ordinance on Amendments to the Ordinance on the manner and timelines for the implementation of security and integrity measures for networks and services</td>
</tr>
<tr>
<td></td>
<td>Regulation on Organizational and Technical Standards for Connecting to the State Information Infrastructure</td>
<td>Regulation on Organizational and Technical Standards for Connecting to the State Information Infrastructure</td>
</tr>
</tbody>
</table>

\(^{47}\) The Ministry of Defence of the Republic of Croatia
In the Republic of Croatia, the concept of information security, measures and standards of information security, information security areas, and the competent bodies for issuing, implementing and monitoring the measures and standards of information security are established by the Information Security Act48. While the Regulation on Information Security Measures was adopted by the Government of the Republic of Croatia at a session held on April 18, 2008.49.

6.2. THE RIGHT TO ACCESS INFORMATION

Democratization of the Society in the 1990s has led to the emergence of a new legislative framework known as the right to access information. The purpose of this new legislative framework was to bring the balance of the requirements of the state administration for classification, ie closing data and public demands for greater openness and transparency of state administration work. Thus, the Council of Europe of 27 November 2008 adopts the Convention on Access to Official Documents opened for signature by Council of Europe member states on 18 June 200950, and it has not yet come into force, and when it comes into force will be the first international binding document on the right to access to information.

In Croatia, the right of access to information is a fundamental human right protected by the Constitution of the Republic of Croatia51, The European Convention on Human Rights and

48 Official Gazette 79/07
49 Official Gazette 46/08
50 The Croatian Law on Access to Information currently does not meet three of the six minimum standards listed in the Convention. Namely, public authorities in Croatia may charge administrative fees for each request for access to information, irrespective of the way information is provided (hence, for personal insight into documents). In addition, the law does not provide for a test of public interest and the test of propensity prescribed by the Convention. In addition, the appeal process and the lawsuit to the Administrative Court for citizens is lengthy (the total duration is 6-8 months), and in the case of a negative solution, citizens have to pay 1000 kuna of court costs.
51 Ĉl.38.st.4. They are guaranteed the right to access information held by public authorities. Restrictions on the right of access to information must be proportionate to the nature of the need for restriction in each individual case and necessary in a free and democratic society and are prescribed by law. (Official Gazette 56/90, 135/97, 8/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14)
The right of access to information is the right of the user to seek and obtain information of public character, including the obligation of the public authority to provide access to the requested information or to disclose information irrespective of the request made when such disclosure arises out of the obligation prescribed by law or other regulation.

According to the Convention on the Right of Access to Official Documents, it sets minimum standards that should be respected by all member states of the Council of Europe, including:

- The Convention establishes the right to request official documents that are defined very broadly, as any information held by the public authority in any form;
- the right to access information may be requested by any person without the need to prove a particular interest in obtaining information;
- States should not impose a charge on filing the application itself and personal insight into documents;
- the right to information access refers to all public administrative bodies, and states may choose to apply both to the legislative body and to private bodies performing public functions;
- there is a limited list of exceptions (12 in total) in which cases information may be refused, which must be subject to a test of public interest and a test of proportionality;
- applicants are entitled to a speedy and inexpensive appeal procedure and must have the right to refer to the court or other independent body.

The Convention prescribes that formalities about obtaining information must be kept to a minimum and requests processed promptly. Public authorities should take into account the

---

52 Čl.10.st.1. Everyone has the right to freedom of expression. This right includes the freedom of opinion and the freedom to receive and disseminate information and ideas without interference with public authority and regardless of frontiers. This article does not prevent States from subjecting the licensing regime to institutions performing activities of radio or television and cinematographic activities. (Official Gazette, International Agreement 18/97, 6/99, 14/02, 13/03, 9/05, 1/06, 2/10)

53 Official Gazette 25/2013, 85/2015

54 Currently, it is conducting a campaign to sign conventions in European states to help the state demonstrate its support for the right to access information.
information they possess and educate officials about their duties and responsibilities with regard to providing information\(^{55}\).

What is important to note is that the right to access information does not mean losing the power of control of state administration, but in contrast to this new legislative framework, the state administration further controls the access to data, i.e. it controls the public. Thus, the legal principle of the right to access information includes the possibility of access to some state administration documents or obtaining information on a particular topic, but all under prescribed conditions. This principle includes all data except classified information for which the right to inspect or prohibit it depends on the interdependence between public interest and the protection of values that are classified by a certain data protection, such as national security. In the Republic of Croatia, this problem solves the Privacy Act\(^ {56}\) in its art. 16. which lays down the obligation of the owner of classified information, which is of public interest to carry out the assessment of the proportionality of the two conflicting interests of secrecy and the public, and that, within that process, the National Security Authority (NSA) the central state security information body.

Classified data is defined in Article 2 of the The Privacy Act as the one that the competent authority in the prescribed procedure marked and determined the level of confidentiality. The Privacy Act, in Article 13, cites officials who can perform classification of data to certain degrees of secrecy as follows:

- Classification of data to the degree of secrecy of "HIGH SECRET" and "SECRET" can be carried out by the President of the Republic of Croatia, the President of the Croatian Parliament, the Prime Minister of the Republic of Croatia, the Ministers, the Chief State Attorney, Chief of the Armed Forces Chief of Staff and the heads of the Security and Intelligence System of the Republic of Croatia, they are authorized to do so in writing, solely within their scope.

- the classification of data to the degrees of confidentiality "CONVINCED" and "LIMITED", in addition to persons authorized to classify the degree of secrecy "GREAT SECRET" and "SECRET", may be executed by the heads of other state bodies.

---


\(^{56}\) Official Gazette 79/07, 86/12
these persons classify the data for scientific institutions, institutes and other legal entities when working on projects, inventions, technologies and other matters of security interest to the Republic of Croatia.

It is important to note that the classified data and the one designated by the Republic of Croatia have been submitted by another state, international organization or institution with which the Republic of Croatia cooperates. Then we are talking about international classified information.

6.3. NATIONAL SECURITY STRATEGY OF THE REPUBLIC OF CROATIA

The National Security Strategy is a key security document dealing with the development, implementation and coordination of national power instruments to achieve national security goals. It is a public document provided for by Article 81 of the Constitution of the Republic of Croatia, adopted by the Croatian Parliament and constitutes a political and legal starting point for legislation in the field of national security and defense.

The Republic of Croatia has adopted a total of three national security strategies. The First National Security Strategy of 2002 was in effect until 2017, when a new National Security Strategy of the Republic of Croatia was adopted in the Croatian Parliament.

In the National Security Strategy of 2002 there was no mention of cyber space, actually cyberattacks, what is already identified in the first strategy is the risk of abuse of private data of citizens of the Republic of Croatia by state bodies and institutions of the Republic of Croatia or private organizations. It also recognizes the possibilities of endangering the IT system of the Republic of Croatia in continual increase in the use of IT in the public and private spheres, followed by constant increase in the risk of computer crime and endangering information systems. In the new strategy, the same problem is recognized as "Cybercrime is on the rise, and cyber space is increasingly used for illegal activity. In addition to possible violations of the security of classified, personal and sensitive data, the threat is also the use of cyber space to cause victims and damage to the material world. Radical ideas and movements, which evolve

57 Official Gazette 32/02
58 Official Gazette 73/17
into extremism and terrorism, are multiplying and wider on the internet and social networks, thus gaining reach and influence as they did not have before."\(^{59}\)

The strategy also states that "the Republic of Croatia will develop measures to strengthen the resistance of information and communication systems in the cyber space, as well as reduce the negative consequences of their endangering or disabling. The focus will be on key systems for the normal functioning of state institutions, storage, transmission and exchange of classified and personal data of citizens."\(^{60}\)

Given the character of contemporary international relations marked by the increasingly marked elimination of the boundaries between internal and external security and internal and external policy, and in which foreign policy is increasingly united with elements of security policy, it is necessary to have a flexible national security strategy in which the tasks and capabilities instead of mere focus on threats. The national security strategy is primarily the result of a public policy that applies to all citizens, not just the narrow circle of professionals they are required to implement. Therefore, in defining the concept of national security, civil experts and the private sector should be involved, with the exception of competent state bodies, which implies their interaction and close cooperation in response to general security challenges and concrete forms of endangering national security. Each group understands national security in a way that is appropriate to the goals it advocates\(^{61}\).

6.4. INFORMATION SECURITY INSTITUTIONS IN THE REPUBLIC OF CROATIA

The Office of the National Security Council (UVNS) is the central state security information body - Croatian (NSA) National Security Authority. In this regard, the Office coordinates and coordinates the adoption and monitoring of the application of security measures and standards in the field of security, physical security, data security, information security systems and business cooperation security and issues certificates for natural and legal persons for access to national, NATO and EU Classified Data.

---

\(^{59}\) National Security Strategy of the Republic of Croatia, III Security Environment, Global Level, Official Gazette 73/17

\(^{60}\) National Security Strategy of the Republic of Croatia, IV. Strategic objectives, instruments and mechanisms of their experiments, Development of citizen-level governance and strategic communication, Official Gazette 73/17

\(^{61}\) Siniša Tatalović, Does Croatia need a new national security strategy?, Political analyzes, no. 6 - June 2011.
The Central Registry has been established in the Office, which is responsible for receiving and distributing international classified information and for coordinating the work of the Registry System in state bodies in the Republic of Croatia that receive international classified information. As the NSA body, the Office carries out and coordinates international cooperation in the area of information security and the Government decides on behalf of the Republic of Croatia to conclude international security agreements for the protection of classified information.62

Information security measures and standards relate to staff security checks, physical security, data security, information system security, and security of external co-operation. The Office of the National Security Council prepares annual and extraordinary reports on its work, as well as annual, regular and extraordinary reports on expert oversight of security intelligence agencies (SOA and VSOA) and the OTC Operational and Technical Center for Telecommunication Supervision (OTC).

Information Systems Security Office (ZSIS) is a central state body for performing tasks in the technical areas of information security of the state bodies of the Republic of Croatia, which include information security systems standards, security accreditation of information systems, management of cryptomatic materials used in the exchange of classified information

62 http://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa

Although the focus on data in digital form, the security of the information system also includes data protection on other media, such as paper. The protection applies equally to written and spoken information. Information security management is implemented throughout the life cycle of the information system.

The Department provides comprehensive data protection and information risk management, which implies the application of information security measures in information systems planning and implementation, business continuity, daily logging and threat analysis. Good engineering practice is based on international standards such as ISO / IEC 27002, ISO / IEC 15408, CobiT and the European Union and North Atlantic Treaty Organization (NATO).

In addition to the aforementioned tasks, it carries out research, development and testing of technologies designed to protect classified information and to regulate the technical standards of information systems security. Standards of technical information security areas apply to all state bodies, local and regional self-government units as well as to legal entities with public authority using classified and unclassified data. For the work of accreditation of information systems cooperates with the Office of the National Security Council, while for the activities of prevention and protection and the development of recommendations and standards related to the security of information systems cooperates with National CERT.

**CARNet (Croatian Academic and Research Network)**, Academic Academic and Research Network; is part of the world's computer network in the Internet. In 1995, the Government of the Republic of Croatia by Regulation establishes the CARNet institution. The goals of this institution are: construction and support of computer and information structures of science and higher education; Implementation and support for the experimental work of the latest computer communication and information technologies (IT) and systems; experimental IT applications in various activities, popularization and promotion of mass IT applications in various areas and activities in the Republic of Croatia. The CARNet connection from the Internet

---

²³ [https://www.zsis.hr/default.aspx?id=13](https://www.zsis.hr/default.aspx?id=13)
is based on TCP / IP\textsuperscript{64} protocol, and is implemented through computers in institutions that are members of CARNet. In 1993, Croatia received its .hr top-ranking domain, marking the Croatian site's web site, and top-level domain managed by CARNet. CARNet established a central WWW server in 1994 (the hyperlinks on the Croatian site) and maintains the first internet course for users. Today, CARNet provides ISP services to scientific and educational institutions and their users, takes care of the top .hr domain and carries out many projects to improve content and services in the Croatian internet space.

\textbf{Nacionalni CERT (Croatian national computer emergency response team)} was established in accordance with the Law on Information Security of the Republic of Croatia\textsuperscript{65}. Accordingly, one of the tasks is the processing of incidents on the Internet, ie preservation of the information security of the Republic of Croatia. CERT is a separate organizational unit set up in the Croatian Academic and Research Network (CARNet). The mission of the National CERT is prevention and protection from computer threats to the security of public information systems in the Republic of Croatia. Proactive and reactive measures are being implemented within its scope. Proactive measures are used to prevent or reduce potential damage before the incident and other events that may pose a threat to the security of information systems. Reactive measures have an impact on incidents and other events that can endanger the computer security of public information systems in the Republic of Croatia. Such measures include: Creating and publishing security alerts, collecting, processing and preparing security recommendations on information systems weaknesses, publishing and storing them in their information system, and organization of resolving major incidents involving at least one party from the Republic of Croatia.

\textsuperscript{64} \textit{Transmission Control Protocol (TCP/IP Protocol)} – a set of communication protocols used by computers while working and communicating over the Internet, regardless of the hardware and software platform used. It is a protocol for communication of various types of computer networks. It was developed in the mid-1970s and began to be applied in 1982 replacing the former NCP (\textit{Network Control Protocol}, 1970.)

\textsuperscript{65} Article 20., Official Gazette 79/07
Graph 4. The number of incidents on servers, chart by amcharts.com, source: [https://www.cert.hr/sru/](https://www.cert.hr/sru/), made by: Petra Baničević

The Croatian Personal Data Protection Agency was founded on the basis of the Personal Data Protection Act[^66] which, within the scope of public authority, oversees the implementation of the protection of personal data and points out the perceived abuses in the collection and processing of personal data, compiles a list of States and international organizations that have the proper regulated personal data protection and addresses the request for determination of violations of the rights guaranteed by this Act. In the Republic of Croatia, personal data protection is secured to every natural person regardless of citizenship and residence and irrespective of religious and anthropological differences. The main tasks of the Personal Data Protection Agency are to effectively fulfill all rights and obligations in the area of personal data protection imposed by the Republic of Croatia as a full member of the European Union and the Council of Europe, increasing the accountability of all participants in the processing of personal data related to the application of regulations covered by the legal framework for the protection of personal data in the Republic of Croatia with the appropriate application of information security measures. The Agency also has a permanent task to raise awareness among all participants and all targeted public about the importance of protecting personal data, their rights and obligations, and proposing measures to improve the protection of personal data.

[^66]: Article 27. st.1., Official Gazette 103/03
7. HIGH-PERFORMANCE COMPUTING

HPC (High-Performance Computing) is a strategic resource for Europe's future as it allows researchers to study and understand complex phenomena while allowing policy makers to make better decisions and enabling industry to innovate in products and services. HPC is part of a global race. Many countries (USA, Japan, Russia, China, Brazil, India) have announced ambitious plans for building the next generation of HPC with exascale performance and deploying state-of-the-art supercomputers.

On March 23, 2017, seven European countries signed an agreement to start a European HPC programme that will eventually lead to European exascale supercomputers called EuroHPC. The original EuroHPC declaration was signed in Rome by France, Germany, Italy, Luxembourg, the Netherlands, Portugal and Spain. Meanwhile 15 countries have joined EuroHPC. Croatia is the 13th country to sign the European declaration on high-performance computing (HPC)\(^67\). However, Europe is lagging behind in the field of supercomputing.

As a wide range of scientific and industrial applications will be made available at EU level, citizens will benefit from an increased level of HPC resources in areas like:

- Health, demographic change and wellbeing
- Secure, clean and efficient energy
- Smart, green and integrated urban planning
- Cybersecurity
- Weather forecasting and climate change
- Food security

**Could a future computer or supercomputer run a government?**

A 'supercomputer' refers to a machine which can process information and make calculations so fast it can do complex predictions and modelling. Is it possible to create an algorithm that will put in place the correct and correct laws and policies of human society management is not in question. The complexity of such things is amazing, but I do not doubt it can do that. We have algorithms that can make decisions extremely quickly. How to synthesize all this information in something that can say "this is the law, this is the consequence". I think

this is not a far the future and something that can’t be done. The problem occurs when people are lost in such situations. The question arises where I end up as a human being, and do I start as an algorithm? And whether subhuman humans can leave supercomputers in their hands, regardless of the incoherence of their correctness.

8. CONCLUSION

Although the Republic of Croatia has recognized the problem of personal data protection, there is still room for improving and preventing cybersecurity, as well as cooperation and comparison with other countries. As society relies more on technology, it is important to implement awareness on information protection at the national level. However, this development does not stop. It is subject to constant changes and reviews of existing legislation in the area of privacy protection due to new technological innovations and new social relationships under their influence. Today's citizens expect to receive the necessary information from their governments as quickly as possible. Practice in the world in information and protection of personal data will also be expected from our governments.

Because of this, laws at national level as well as at European level will be changed and adapted to new challenges brought by new technologies.

9. REFERENCES

Siniša Tatalović, Does Croatia need a new national security strategy?, Political analyzes, no. 6 - June 2011.
Klaić, A. Perešin – Concept of regulatory security information framework, 2011.g.
https://www.weforum.org/agenda/2017/01/these-are-the-most-likely-global-risks-2017/
http://www.aaiedu.hr/osustavu/povezani-sustavi/e-gradani
Statistical report 24.02.2016.g., Ministry of Administration
e-Croatia 2020 Strategy, Indicators on the use of public administration services through the Internet for citizens
https://savjetovanja.gov.hr/vijesti/dvije-godine-portala-e-savjetovanja/1157
National Security Strategy of the Republic of Croatia
http://www.uvns.hr/hr/o-nama/djelokrug/informacijska-sigurnost-nsa
https://www.zsis.hr/default.aspx?id=13