Crime prevention policy	
EU- priority	Cybercrime; • Child sexual exploitation • Payment card fraud • Cyber-dependent crimes
Country	Latvia
Year	2018

1. Overview of the field

Definition of cybercrime

Latvian law does not define the concept of "cyber crime" separately, which does not mean that these crimes in Latvia are not criminalized. There is also no uniform definition of cybercrime in Latvian case law and legal doctrine. One of the definitions of cybercrime describes cybercrime as a criminal offense against the security of an automated data processing system - against confidentiality, availability and integrity. Although cybercrime definitions have different views and several debates, there is no doubt that cybercrime is only an offense committed online (on-line)

Cybercrime can be categorized in several ways, for example, according to the object against which the violation is committed:

- offenses against the person (virtual voyeurism, virtual harassment, killing, negligence, murder, etc.);
- sexual crimes (virtual rape, publication of obscene material, crimes against minors, prostitution and related crimes, etc.);
- crimes related to interference and damage to property rights of persons (crimes against security of information systems, etc.);
- theft and fraud (computer fraud and computer theft, etc.);
- moral offenses (supply of alcohol and tobacco on the Internet, gambling, etc.);
- Government-facing crimes (terrorisms, etc.).

In accordance with Latvian legislation, several articles are devoted to cybercrime in the Latvian Criminal Law (Criminal Code). For example, Section 144 of the CL provides for liability for violations of correspondence, information transmitted over a telecommunications network and other information secrets (one example could be the modification of e-mail correspondence, connection to foreign e-mail). The specific offense is directed towards the fundamental rights and freedoms of a person.

Fraud is regulated in clause 177.1 of the Criminal Code. It should be noted that computer fraud should not be confused with ordinary fraud, for which liability is provided for in Clause 177 of the CL. A scam is a different offense for the offense. The target of computer fraud is a computer system, not a person as a traditional fraud. Computer fraud, like ordinary fraud, also falls within the category of criminal offenses against property.

Section 193.1 of the CL provides for criminal liability for obtaining, producing, distributing, using and storing data, software and equipment for illegal activities with financial instruments and means of payment. This is a criminal offense in the national economy.

Article 241 of the Criminal Law provides for criminal liability for arbitrary access to an automated data processing system. Article 243 of the CL provides for criminal liability for interrupting the operation of an automated data processing system and for unlawful handling of information contained in this system. Section 244 of the CL provides for criminal liability for unauthorized activities with devices for influencing the resources of an automated data processing system. Article 244.1 of the CL - on the acquisition, production, modification, storage and distribution of data, software and equipment for the illegal operation of electronic communication network terminals. It is important to point out that Articles 241-244.1 of the CL as an object of a crime group constitute an offense against general security and public order.

Criminal offenses related to violations of personality and sexual integrity committed through the use of information and communication technologies are not directly separated from the crimes of this kind that have not been committed using this channel in Latvian legislation. Consequently, special attention is paid to the following Articles of the Criminal Code:

1. Article 162 of the CL and its parts, and Article 162.1 and its parts (Obligatory admission and Encouragement to engage in sexual activities (in particular against a minor))

2. Clause 166 of the CL and its parts (Violation of the rules for the display of a pornographic performance, intimate entertainment and pornographic material circulation (in particular against a minor))

Assessment of trends and developments

As information technologies evolve, potential offenses in the online environment also develop. The safest way to reduce the damage done online is for the individual to care for itself. Consequently, it is necessary to continuously educate the public on how to protect oneself. The main tasks of CERT.LV are to maintain and update information on IT security threats, provide support to state institutions in the field of IT security, provide support for the prevention of IT security incidents for any physical or for a legal person, if the incident involves Latvia's IP address or the .LV domain, to organize information and education measures for both government officials, IT security professionals and other interested parties. However, online threats also apply to any Internet user. The State Police are involved in rare cases. Those are mostly cases of sexual abuse and fraud.
In 2017, as one of the priorities of the State Police, the fight against crimes against the integrity of the juvenile and adolescent and the sexual immorality of offenders, including the fight against crimes involving the dissemination of child pornography through information technology, has been identified.
According to the Criminal Law and the Criminal Statistics Report of the Information Center of the Ministry of the Interior for 2017, the following types of crimes can be identified, which should be intensified:

3. (Section 162 of the KL and its parts, and Article 162.1 and its parts) Conduct of fornication and Encouragement to engage in sexual activities (in particular against a minor) and (Section 166 of the CL and its parts) Pornographic play demonstration, intimate entertainment restraint and pornographic Violation of the rules of material circulation (in particular against the minor);
4. (Clause 177 (1) of the CL) Personal fraud, abuse of trust.

Recent overview of statistics and research

The Preventive Control Department uses in its work the research carried out by various institutions on current issues.
During the period from October 2017 to November 2017, the Department of Mediation of the University of Latvia, supported by the Ministry of Culture of the Republic of Latvia, carried out a study on the mediation of Children and adolescents (9-16 years old). The survey included 1203 children and adolescents from 9 to 16 years of age throughout Latvia. The results suggest that some children and adolescents lack the knowledge and skills necessary to use them safely and skillfully, create and share various types of information. Such a lack of knowledge can be the basis for committing a criminal offense in which a minor can be both a perpetrator and a victim.

Below you can see the number of cases registered at the State Police according to the data of the Information Center of the Ministry of the Interior.

	2015	2016	2017
Section 162. Leading to Depravity (1) For a person who commits leading to depravity of a person who has not attained the age of sixteen years or who is in the state of helplessness, that is, for a person who commits acts of sexual nature without physical contact with the body of the victim for the purpose of sexual gratification or to rouse sexual instinct in the victim, if such act has been committed by a person who has attained the age of majority or it has been committed taking advantage of the state of helplessness of the victim or against the will of the victim by means of violence, threats or using trust, authority or exerting other influence over the victim. (2) For a person who commits the criminal offence provided for in Paragraph one of this Section, if it has caused serious consequences, or it has been committed on a minor.	107	45	42

Section 162.[1] Encouraging to Involve in Sexual Acts (1) For a person who encourages a person who has not attained the age of sixteen years to involve in sexual acts or encourages such person to meet with the purpose to commit sexual acts or enter into a sexual relationship using information or communication technologies or other means of communication, if such act has been committed by a person who has attained the age of majority. (2) For a person who commits the criminal offence provided for in Paragraph one of this Section, if it has been committed on a minor.	**18**	**13**	**21**
Section 166. Violation of Provisions Regarding the Demonstration of a Pornographic Performance, Restriction of Entertainment of Intimate Nature and Handling of a Material of Pornographic Nature (1) For a person who commits violation of the provisions regarding demonstration of a pornographic performance or other provisions regarding the restriction of entertainment of intimate nature, or provisions regarding the handling of a material of pornographic nature, if it has been committed on a significant scale or substantial harm has been caused by committing it. (2) For a person who commits visiting or demonstration of such pornographic performance or handling of such materials of pornographic nature which contain child pornography, sexual activities of people with animals, necrophilia or sexual gratification in a violent way. (3) For a person who commits encouraging, involvement, forced participation or utilisation of minors in a pornographic performance or the production of a material of pornographic nature. (4) For a person who commits encouraging, involvement, forced participation or utilisation of persons who have not attained the age of sixteen years in a pornographic performance or the production of a material of pornographic nature.	**226**	**313**	**160**
Section 177. Fraud (1) For a person who commits acquiring property of another, or of rights to such property, by the use, in bad faith, of trust, or by deceit (fraud).	**794**	**704**	**599**

Other national priorities besides child sexual exploitation, payment card fraud and cyber-dependent crimes?

The Latvian Cybersecurity Strategy 2014-2018 has been approved at the national level, which states that it is essential to develop a comprehensive set of measures protecting the cyber location and its services in order to mitigate the damage to the public through ICT. These tasks for implementation in the strategy set five priority directions of action:

1. Cybersecurity management and resources;
2. Justice in cyberspace and cybercrime alleviation;
3. Public awareness, education and research;
4. Readiness and capability in crisis situations;
5. International cooperation.

Combating cybercrime is one of several priorities of the State Police in the period 2017-2019.

In Latvia, high-tech offenses (cybercrime) are mostly fought by the GKRPP Economic Crime Combating Bureau, Section 3, which employs 20 officials. The Section has put forward several areas of action:

1. Security (availability, confidentiality, integrity) of automated data processing systems (ADPS) for online threats;
2. Use of ADPS for online data security threats;
3. Infringements in the field of copyright and related rights;
4. The use of illegal software for commercial purposes;
5. Illegal television distribution;

6. Infringements in the field of industrial property rights;
7. Illegal activities in the field of electronic payment systems:
• Illicit use, distribution and production of counterfeit, illegaly acquired electronic means of payment;
• The acquisition, distribution and use of data, software and equipment for illegal activities with electronic payment instruments, incl. internet environment.
8. Violation of online pornographic material circulation rules that describe or depict the sexual exploitation of children, human sexual activity with animals, necrophilia or pornographic violence.
Together with these priority tasks, cybercrime prevention is planned. Given that prevention in this field, which is aimed at legal entities is more complicated, it is mainly focused on the individual within the mentioned directions.

2. Crime strategy and coordination

Objectives of the crime strategy

Objectives and tasks of combating cybercrime are set out in the rules of the Section (Section 3 of the Economic Crime Combating Bureau of the GKrPP).
1. Plan, coordinate and take measures to prevent and detect criminal offenses and other offenses related to
1.1 the security (availability, confidentiality, integrity) of automated data processing systems (hereinafter - ADPS) for online;
1.2 use of ADPS for online data security threats;
1.3. Illegal activities in the area of electronic payment systems, i.e .:
1) the illegal use, distribution, production of counterfeit, alien, alienated electronic means of payment;
2) the acquisition, distribution and use of data, software and equipment for the illegal activities of electronic payment instruments, incl. internet environment;
1.4 Violation of pornographic material circulation rules online that describes or depicts the sexual exploitation of children;
1.5 protection of intellectual property (including illegal distribution of audiovisual content);
2. conducts preliminary investigation and preliminary investigation of criminal proceedings according to the competence of the department;
3. Performs Internet monitoring within the scope of competence;
4. performs operational analysis in criminal cases and operational accounting cases, analysis of crime status, incl. carries out criminal intelligence in the areas competent for the department;
5. coordinates and supervises the work of the territorial police departments of the State Police, as well as provides methodological and practical assistance in these areas.

Role of prevention in the crime strategy on state/regional/local level

More and more forms of communication are emerging between people through different information and communication technologies. Online communication brings people together because they provide the ability to share information, including pictures. People are keen on taking advantage of this opportunity and sharing intuitive information and pictures without considering the consequences. If it seems unsafe during a conversation, then after a deterioration of the relationship, there is a risk of misuse of previously received pictures, namely, distribution on social networks or sharing with other people.
Online communication also expands the opportunities to meet new people. Given the apparent anonymity in the online environment, this form of communication is also abusive. Perpetrator obtains victim confidence, emotionally brings himself closer to victim and being interested in continuing communication. Thus, the victim is called to reveal his secrets and send pictures that are later used for blackmail. State Police officers are faced with situations where the perpetrator is not located in Latvia at all, so it is impossible to completely eliminate the consequences of the crime.
The crime is not seasonal or "hot spot". However, for all types, there is a lack of awareness and uncertainty among the victims. Essentially, it must be admitted that the level of crime is largely determined by the carelessness of the involved, the lack of understanding about the possibilities of information technology. This means that the emphasis should be on informing people.
In order to minimize sexual offenses in the online environment as well as to stop sexual abuse in the Internet, before it is committed in the face of sexual abuse, it is necessary to focus on

preventive work to address the following problems or reduce their risks:

A. Unawareness of the consequences of sending nude pictures;
B. Unawareness of the consequences of transferring nude pictures;
C. Ignorance of risk in contact with a stranger;
D. Failure to report "harassment" on the Internet to the police.

The main emphasis is on following target audiences / preventing or reducing the risks mentioned above: children and adolescents, young people who spend a lot of time on a daily basis spend a lot of time in social networking applications, their parents.

Fraud in the online environment is manifested in the impact of one person or group of people on an individual. Initially propitiating, a person's confidence, grace it is later abused with blackmail and manipulation. The perpetrator from an individual acquires the desired one:

- sexual information;
- money and other financial benefits.

Such abuse is a threat to the person's personal data that the naive person shares with the trusted conversation partner. This phenomenon must be fought in the minds and at the disposal of the victim, because in the majority of cases, the scandal of funds and data is in another country that is no longer under the jurisdiction of Latvia.

In order to minimize individual fraud in the online environment, it is necessary to focus on preventive work on educating potential victims about the specifics of the crime, so that they can recognize the signs of a criminal offense in a timely manner.

The main emphasis is placed on the following target audiences / prevention or reduction of the above-mentioned issues - young people and adults seeking an affiliate online.

Implementation of the policy (which level is responsible for the implementation and how is the implementation coordinated?)

Prevention of the State Police of Latvia is implemented at several levels. Crime prevention unit operates at the state level managing analytical work, programs and interventions, developing and coordinating actions for regional and local-level tasks.

The structure of the State Police of Latvia is divided into 5 regions. There are 5 units responsible for regional interventions and solving problems that are relevant only to a particular region and coordinating local police station work at regional level.

Also there are 41 State Police stations in Latvia and over 100 juvenile inspectors are employed. The State Police juvenile inspectors are responsible for the juvenile crime prevention.

In co-operation with the 3rd Section of the Economic Crime Prevention Department of the State Police, the Crime Prevention Unit identifies the current situation and trends, thus identifying the necessary actions for the prevention of a criminal offense.

Stakeholders (working groups, specialised agencies, partners, etc)

At the national level, there are several documents related to combating cybercrime and investigation procedures. All institutions that have signed on fulfilling the tasks of these documents are mutual partners. These documents are:

- National Security Concept
- National Defense Concept
- Information Technology Security Law
- State Information Systems Law (Development of MEPRD)
- Latvian Sustainability Development Strategy till 2030
- Information Society Development Guidelines for 2014-2020
- Concept of the organizational model for the management of state information and communication technologies
- Guidelines for the Electronic Communications Industry Policy 2011-2016. year
- Authentication Law (Development of MEPRD)
- Concept of the Cyber Defense unit of the National Armed Forces of the Ministry of Defense, 2013.

Consequently, the institutions and organizations involved in the implementation of these documents are the State Polices Cooperation Organizations for combating cybercrime.

The state police has established a close cooperation with the CERT.LV (Ministry of Defense of the Republic of Latvia) and NET-SAFE LATVIA Safer Intertech Center.

Participation in European/ international networks, working groups, etc.
The State Police collaborate with several cyber security organizations to share expertise, including CEPOL, the European Commission, the General Secretariat of the Council of Europe, Europol, and EMPACT. The International Co-operation Office of the Main Criminal Police Department of the State Police also ensures Latvia's membership in the EU-LISA network.

3. Good practices

Overview of recent good practices, prevention programs, etc.
Each year, the Crime prevention unit of the State police of Latvia develops and implements various informative materials and handouts for various occasions - posters for schools, bookmarks for children, various brochures and even USB flash drives. These materials include tips on how to protect yourself, how to recognize threats and how to handle them. Brochures with tests for parents on how to monitor children's activities on the internet, as well as brochures-tests on how to evaluate your internet habits and make them safer have been developed. Preventive play book for children has been developed. This book includes educational aspects on cyberbulling and internet pornography. The interactive version of the material is available in Latvian at http://www.vp.gov.lv/pasaka/. The State Polices Crime Prevention unit has developed a website www.manadrosiba.lv and a mobile application. The website is regularly updated with clear information and advice on current issues and trends. The information in it is divided according to the actualities of adults and teachers, current issues of specialists in different fields and children of different age groups. The "Bite Yourself in the finger" by communications company “BITE”, which also involves the state police. Within the campaign, children and teenagers are encouraged to use their mobile devices responsibly, without offending others; parents, educators, the media, the public are encouraged not to be indifferent, to recognize cyber mobs and to act. The State Police provides an informative basis on the most common problems, responsibilities and actions in dealing with cyberbullying. There has been a Distribution of Mobile Malware Awareness campaign materials in 2016 (developed by Europol) on various channels, including the website and social media accounts of State police of Latvia as well as other social media platforms and internet media. The materials were also distributed to coordinators in Ministry of Education for distribution in schools all around Latvia. This year On September 27, Drossinternets.lv, the State Police and the Ministry of Culture launched a social campaign "Surveillance on the Internet". The purpose of the social campaign is to promote child mediation and safety on the Internet, informing both children and adults about the risks and opportunities in the Internet environment. Within the campaign five videos have been created that teach children 5-8 years of understanding the various situations they can face on the Internet. Campaign images - The SuperAnna and SuperToms campaign brings children to learn and remember simple basic rules of security and mediation that must be kept in mind for both prospective and current Internet users: • What not to tell a stranger on the Internet? • When to call an adult who trusts? • What can be spoofed on the Internet? • How to behave on the Internet? • How can the Internet help? More information is available at: http://vp.gov.lv/supervaronis/.