SPARTA

D4.5

Cybersecurity Threat Prediction Legal Framework

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1 February 2019,
Duration	36 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D4.5 / V1.0
Work package contributing to the deliverable	WP4
Due date	Jan. 2022 – M36
Actual submission date	11th February, 2022

Responsible Organisation	UBO
Editor	Marc Ohm
Dissemination level	PU
Revision	V1.0

Abstract	Task 4.5 aims to conduct research on new and changing legal phenomena resulting from large data volumes, knowledge management of complexity, and predictive analytics that are characteristic of full-spectrum cybersecurity intelligence.
Keywords	Disinformation, Cybersecurity Regulation, Subcases

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Marc Ohm (UBO)

Contributors (ordered according to beneficiary numbers)

Christina Pavlou (KEMEA)

Sigutė Stankevičiūtė, Olga Navickienė, Mangirdas Morkūnas (LKA)

Regina Valutytė (MRU)

Tun Hirt, Kadri Bussov (SMILE)

Reviewers (ordered according to beneficiary numbers)

Eren Cakmak (UKON)

Marek Pawlicki, Michal Choras, Aleksandra Pawlicka (ITTI)

Executive Summary

The present deliverable (D4.5), the fifth of six, is part of the Work Package 4 (WP4). The latter aims to navigate the applicable legislative requirements in terms of 'T-SHARK - Full-spectrum cybersecurity awareness'. Task 4.5 **'Legal issues analysis and framework development'** will address legal and privacy requirements as a conformity with research challenges. Under this scope, the document will perform legal and privacy analyses on the cybersecurity sector. Specific emphasis will be given, among other legal aspects, in the analysis of applicable legislation on disinformation and cyber security. An additional approach will try to address the developed subcases during the project timeline, conducting an analysis of them from a legislative point of view, offering also a broader overview of the applicable principles and regulations in terms of the project.

Table of Content

List of Figures

List of Tables

Chapter 1 Introduction

Cybersecurity phenomenon is getting a wider scientific and practical focus in recent years and is already acknowledged as even a sort of military hostility by the NATO[1]. One of the main cybersecurity threats in the EU is considered to be possible election interference[2]. Such types of threat are common not only for the EU Member States but also to its NATO allies, such as the US or Commonwealth states[3]. It has even been argued that election interference has taken such a level that it may significantly influence the results of the general election[4]. Therefore, concerns regarding possible election interference in the future in the EU are actually substantiated. Such a situation impedes the possibility of a wider implementation of e-Governance (in particular, e-voting) in most of EU Member States. If implemented, this could contribute to civic participation and citizens' participation in politics, thus strengthening democracy.

It is considered that EU Member States could more effectively respond to and counter the disinformation if acted in a collaborative way[5], which would make a response more multifaceted and even act as a deterrence mechanism to some disinformation spreading subjects that are typically located outside the EU and are directly or indirectly controlled by a hostile state[6]. Although one of the barriers for creating an EU-level action plan for the response to disinformation threats is the lack of harmonisation of legislation considering the election process in all EU member states. This process is even more arduous because the cybersecurity issue is quite a new challenge, and the legislation regarding it is currently evolving and no established practice already exists. Therefore, the objective of Task 4.5 is to perform research on new and changing legal phenomena resulting from large data volumes, complexity knowledge management, and predictive analytics that are characteristic of full spectrum cybersecurity intelligence[7]. This objective is achieved by a detailed analysis of eight case studies covering various aspects of legal regulation deficiencies hindering the implementation of proposed measures to counter cybersecurity in the EU, namely: CESNET investigates the possibility of application of DDoS backscatter traffic detection; INOV proposes the employment of mission-aware impact assessment models to incorporate information from multiple intrusion detection systems in order to lower the susceptibility to cyber threats; a unified control centre for the protection of the critical infrastructure is proposed by LEO; disinformation prediction is revealed by LKA; the possibility to implement an automatic malware scanning is suggested by NASK; the recognition of similarities in criminal behaviour in cyber area is suggested by EUT relying on the repeating habitual patterns of cybercrime; simulation of possible cyber-attacks on a critical infrastructure can also help to identify critical points requiring immediate action. All these components mentioned above constitute an umbrella election interference case covering physical and cognitive environments, which need to be connected by innovative methodological and technological solutions[8]. The actors who play a significant role in the umbrella case are many. Those include political parties, individual candidates, critical infrastructure, media, and the public as an electorate.

[1] Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. Security Journal, 30(4), 1151-1168.
[2] Brattberg, E., & Maurer, T. (2018). Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks (Vol. 23). Washington, DC: Carnegie Endowment for International Peace.
[3] Brown, I., Marsden, C. T., Lee, J., & Veale, M. (2020). Cybersecurity for elections: A Commonwealth guide on best practice.
[4] Keating, V. C., & Schmitt, O. (2021). Ideology and influence in the debate over Russian election interference. International Politics, 1-15.
[5] Durach, F., Bârgăoanu, A., & Nastasiu, C. (2020). Tackling disinformation: EU regulation of the digital space. Romanian Journal of European Affairs, 20(1).
[6] Baumann, M. (2020). 'Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations. Contemporary politics, 26(3), 288-307.
[7] T-SHARK T. 4.5 Workshop on Legal Challenges, https://slidetodoc.com/tshark-t-4-5-workshop-on-legal-challenges/.
[8] SPARTA deliverable 4.1., https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

Chapter 2 Methodology

This chapter aims to elaborate on the process of identifying and analysing existing legal challenges with respect to the prediction of cybersecurity threats. The methodology we applied comprises several steps.

First, existing legal challenges were identified based on real world problems encountered by operational partners of T-SHARK. These problems were based on the underlying legal challenges. The most pressing challenge is used as the foundation for further in-depth analysis. That analysis uses several techniques to portray multiple aspects of the problem in order to allow for a holistic discussion of possible shortcomings and gaps.

2.1 Identification and Selection of Legal Challenges

As Task 4.5 is closely related to other tasks and subcases of WP4, all respective partners were asked to report their legal problems encountered. For this purpose, a template was provided to ensure structured responses (see Appendix).

The collection phase was announced via the WP4 mailing list, and partners were reminded during the biweekly WP4 conference calls. Legal challenges were submitted from September 2019 to the end of December 2019 by email or upload to SVN. The outcome of this process is a set of identified legal problems.

2.2 Selection of the main challenge

Challenges from the collected set are assessed according to three main criteria:

- Does the challenge suit the WP's umbrella case (election interference)?
- Is the legal situation around the challenge unclear/incomplete?
- Is it forward-looking and addresses situations that are likely to accumulate in the future?

The assessment is mainly carried out internally with the partners involved in task 4.5. However, the invitation is extended to all partners in WP4. The outcome of this process is one main challenge that will be used for further analysis.

The legal challenges were collected according to the process defined in Section 2.1. In total, 21 challenges were submitted by various partners of WP4. These challenges were analysed and grouped.

It was possible to abstract these challenges into three 'super challenges':

- Disinformation
- Software, Hardware, and Investments from Foreign (adversarial) Countries
- Privacy Challenges in IoT Environments

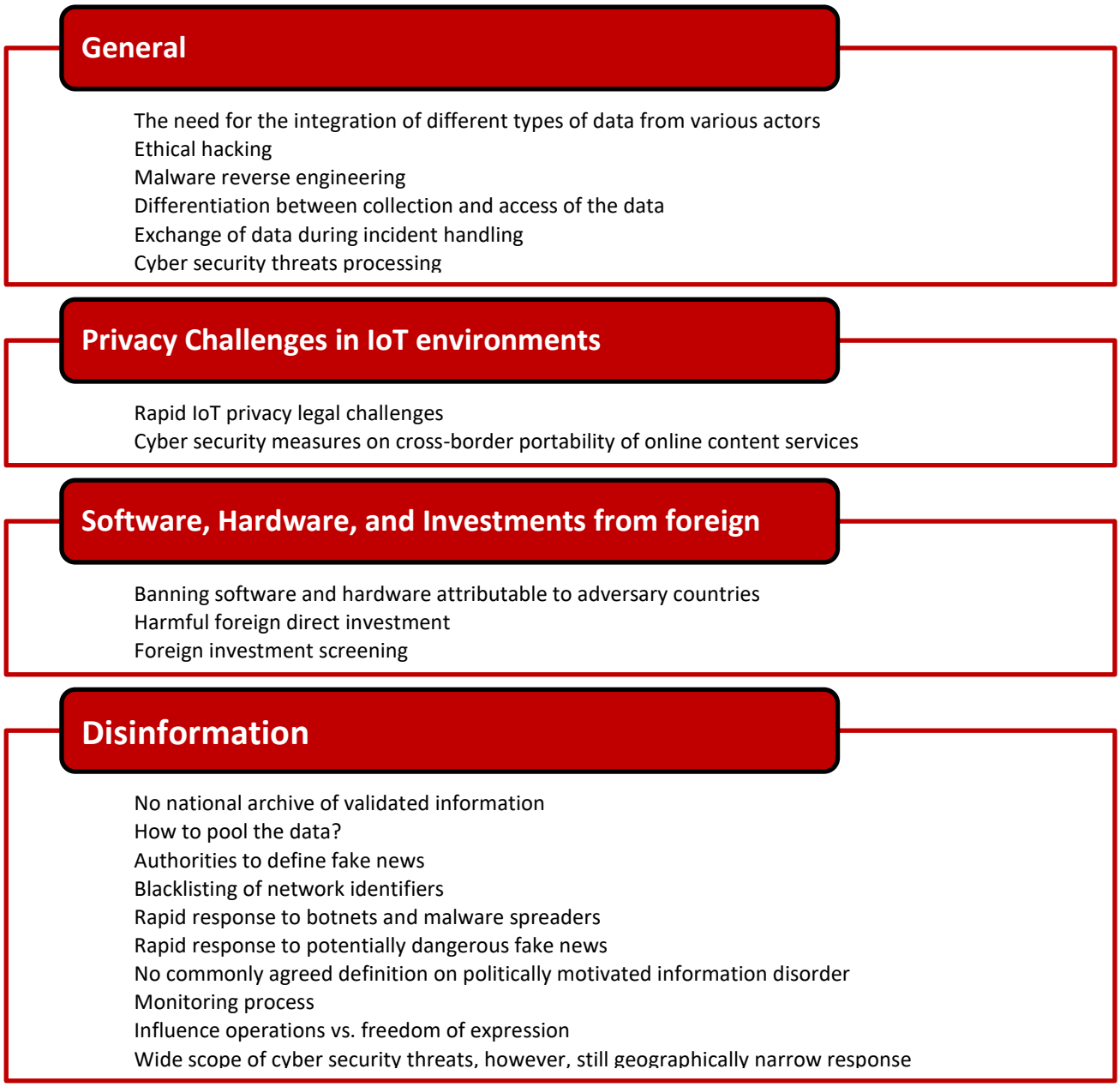


Figure 1: Legal challenges in T-SHARK

During a face-to-face meeting on 14, January 2020, which took place at the General Jonas Žemaitis Military Academy of Lithuania, the super challenges were discussed. *Disinformation* was chosen as the best-fit challenge. Furthermore, it holds the most 'sub-challenges' proposed by partners of WP4.

2.3 Assessment of the State-of-the-Art in Laws

Between January 2019 and January 2021, the impact of disinformation actions and responses to them was considerably different than in previous years. European Parliament research showed that disinformation actions increasingly merged with genuine content and their sources became even more difficult to identify. Particularly strong impacts were observed in cases where disinformation and manipulative propaganda were spread by individuals with high levels of political authority who enjoy the trust and attention of citizens. Diverse legislative and policy measurements were introduced by various member states and third states, and civil society responses also flourished, particularly in relation to increasing resilience against disinformation. Ongoing research into the

psychological mechanism of manipulation and resilience gives more detailed results. This study aims to provide recommendations on legislative and policy measures to protect democracy, the rule of law, and fundamental rights from the impact of disinformation, as well as to create a structured information ecosystem that promotes and protects these values[9].

The questionnaire "On national measures against disinformation" was sent to the different partners of the SPARTA project in order to collect comparative data of the existing national measures against disinformation in different member states of the EU. We received 14 responses, including data on the following countries (in alphabetical order): *Austria, Belgium, Denmark, Estonia, France, Germany, Greece, Ireland, Latvia, Lithuania, Luxembourg, Poland, Spain, and Sweden*. Additionally, the analysis was supplemented by data collected through desk research.

In 2020-2021, several reports and publications were published on the subject of disinformation regulation. The reports covered the implications of disinformation regulation in the European Union on both the right to freedom of expression and the right to privacy[10], the analysis of anti-defamation legal regulation[11], national law of the EU member states applicable to the definitions of disinformation[12]. Given this, WP4.5 researchers reshaped the research to provide the full view on specific legal regulation targeting disinformation in all Member States, in particular, focusing on the law enforcement measures. The analysis also takes into account recent legislative changes adopted to combat the 'infodemic' of Covid-19. The analysis does not cover the measures taken during the wartime. The corresponding results of the survey are discussed in Chapter 3.

The term disinformation for the purpose of this report designates the creation and diffusion of false information (false facts or a misleading presentation of facts) in order to cause harm or make a profit[13], as suggested by European Commission. This term disinformation was chosen here, but different related terms exist and designate similar phenomenon: fake news, malinformation, misinformation, propaganda, etc.

Since disinformation topic is already widely addressed in the research from the human rights perspective, the instrument of moot court, a simulated court hearing, was chosen to simulate the strengths and weaknesses in legal argumentation in case a state decides to enforce legal measures in fighting disinformation. To conduct such moot courts, MRU organized two internationally represented sessions in which legal cases were discussed. The hypothetical scenario (moot problem) as well as the results of the moot court can be found in the appendix.

2.4 Legal issues related to cybersecurity threat prediction in T-SHARK subcases

Lastly, the subcases developed in T-SHARK are analyzed for legal issues related to cybersecurity threat prediction. This analysis is two-fold.

First, a general framework of laws regarding Cybersecurity & Information Systems Security, as well as Data Protection and Privacy Regulation, is set up. This is followed by an in-depth analysis of each

[9] European Parliament. Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States. https://www.europarl.europa.eu/thinktank/fr/document/EXPO_STU(2021)653633.

[10] Hoboken, J., Fathaigh, Ó R. (2021). Regulating Disinformation in Europe: Implications for Speech and Privacy, 6 UC Irvine Journal of International, Transnational, and Comparative Law, 9, https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1041&context=ucijil, p. 20

[11] Scott, G. (2017) Defamation and Insult Laws in the OSCE Region: A Comparative Study, https://www.osce.org/files/f/documents/b/8/303181.pdf

[12] Ronan, Ó F., Helberger, N., Appelman, N. (2021). "The perils of legally defining disinformation". Internet Policy Review 10 (4), https://policyreview.info/articles/analysis/perils-legally-defining-disinformation

[13] A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation, 12 March 2018, p.11, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271

subcase. To get a concise description of each subcase, all subcase owners in T-SHARK were asked to fill in a template describing their subcase.

The template was again distributed via email, and partners were reminded to fill in during the biweekly WP4 conference calls. The information provided was used as the basis for legal analysis. Uncertainties were clarified in bilateral conference calls with the responsible partner. The results are discussed in Chapter 6.

Chapter 3 State of Play in Legal Regulation of Disinformation in the EU

3.1 Mapping Legislative Measures and Regulatory Initiatives

The analysis of the data collected allows for grouping the countries based on the types of actions they have taken. Favouring a less restrictive approach on the exercise of the right to freedom of expression, some countries take non-binding actions, and other states are looking for legislative solutions. The data collected led to the distinction of the Member States into three main groups.

The first group represents the countries that have adopted legislation relevant to fighting disinformation. This group also includes the Member States that did not create any specific regulation to combat disinformation; they use the existing legal framework instead. The group includes 15 EU member states, such as *Austria, Croatia, Cyprus, Denmark, France, Germany, Greece, Italy, Lithuania, Portugal, Romania, Hungary, Malta, Latvia, and Spain*. It must be noted that those countries also take non-legislative measures.

Austria, Croatia, Cyprus, Denmark, France, Greece, Hungary, Italy, Lithuania, Malta, Portugal, Romania already have a specific legislation to combat disinformation; however, the scope and nature of the legislation differ in each country. *Denmark, Austria, Poland, France, and Spain* focus on the protection of democratic processes, in particular elections. *Lithuanian* law on 'The Provision of Information to the Public' targets disinformation and gives the power to the Lithuanian Regulator for Audio-Visual Content (LRTK) to suspend broadcasting or impose fines on broadcasting services. *Portugal* gives the power to the Media Regulatory Authority to assess complaints against any person who performs the acts defined as disinformation and applies the sanctioning regime. *Greece* prohibits 'false news' that causes concern or fear in the public or undermines public confidence in the national economy, the country's defence capacity, or public health.' Similarly, *Cyprus* prohibits any form of false news that can cause disturbance of public order or public confidence in the state or its authorities, or cause fear or anxiety in the public, or in any way disrupt the common peace and order by means of criminal law. *Croatia* establishes a general prohibition of invention or the spread of false news that disturbs the peace and tranquillity of citizens as a misdemeanour. *Germany* seeks to improve the enforcement of the law in social networks and places the burden on platform providers to remove illegal content. *Latvia* does not have any regulation specifically targeting disinformation in force; however, it applies other criminal law provisions to combat the phenomenon.

The second group represents the countries that intended to adopt legislation but did not succeed or are in the process of adopting a regulation. After unsuccessful attempts to amend the Criminal Code and the Radio and Television Act in 2020, *Bulgaria* intends to change the Personal Data Protection Act. In the Progress Report of the Interdepartmental Group on the Security of Ireland's Electoral Process and Disinformation (IDG)[14], *Ireland* took an approach similar to France and intends to regulate online political advertising within the election period and reform the funding of election and referendum campaigns. It must be noted that those countries also take non-legislative measures.

The third group represents the countries, which *take a non-legislative approach* by taking soft measures such as educative programmes, media literacy activities, task forces, monitoring, support of the research, etc. It includes 10 countries: *Belgium, Czech Republic, Estonia, Finland, Luxembourg, Netherlands, Poland, Slovakia, Slovenia* and *Sweden.* Countries fear that regulation of disinformation may result in censorship. Measures can concern increasing media literacy through educational programs: reform of schools' programs to include digital media literacy courses or other media literacy actions through Internet portals, government campaigns, etc. Finally, measures can

[14] Online Political Advertising in Ireland: Regulation of Transparency. https://www.gov.ie/en/policy-information/7a3a7b-overview-regulation-of-transparency-of-online-political-advertising-/

be the implementation of an executive unit or task force, sometimes as the implementation of the EU action plan, or sometimes as government initiatives.

3.2 Case studies of disinformation in European Union

3.2.1 Austria

Although Austria is classified among countries that continue largely to ignore or deny the existence of Russian disinformation and hostile influence operations[15], Austria changed the Criminal Code in 2019 to criminalize the dissemination of false information during an election or referendum. Article 264 of the Criminal Code was modified for this purpose. The provision prohibits the public dissemination of false information about circumstances that may prevent voters from voting or exercising their right to vote at that time, when the retaliation campaign is ineffective in terms of time. The criminal act is punishable by imprisonment for up to six months or a fine of up to 360 days. If someone uses a false or forged document to make a false communication appear to be credible, the criminal act is punishable by a term of imprisonment of up to three years [16].

3.2.2 Belgium

On 30 November 2021, no legislative measures were adopted in the country that would be directly relevant to counter disinformation. The country *takes a non legislative approach* by taking soft measures such as educational programmes, media literacy activities, monitoring, support of the research, etc.

3.2.3 Bulgaria

On 30 November 2021, no legislative measures were adopted in the country that would be directly relevant to counter disinformation. In response to the COVID-19 'infodemic', there have been three attempts in Bulgaria to change different laws and punish spreading disinformation.

As in a number of other European countries, there have been attempts in the country to apply the criminal law provision, the main function of which is to penalize those who make false bomb alerts, abuse police, fire brigade, and ambulance workers by calling them without the need for their assistance. Article 326 of the Bulgarian Criminal Code criminalises a transmission over the radio, by telephone, or in some other way false calls or misleading signals for help, accident, or alarm. The criminal act is punished by imprisonment for up to two years and, in case there are considerable harmful consequences, by imprisonment for up to five years and a fine from BGN five hundred to two thousand[17]. Despite criticism for an over-extended interpretation of the provision, the Prosecutor's Office tried to seek responsibility from various persons based on this article[18].

The emergency bill vetoed in March 2020 by the President of the Republic of Bulgaria proposed the amendment to the provision by expanding the scope of the criminal act and criminalizing a transition 'through radio, telephone, or other means, false information on the spread of infectious diseases'. If

[15] Kremlin Watch Report, 16 May 2017, Overview of countermeasures by the EU28 to the Kremlin's subversion operations. How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies? P. 11, 28, https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf

[16] Criminal Code of the Republic of Austria, https://www.legislationline.org/download/id/8548/file/Austria_CC_1974_am122019_de.pdf

[17] Criminal Code, https://www.legislationline.org/documents/action/popup/id/8881/preview.

[18] AEJ Bulgaria, Criticizing Anti-Pandemic Measures and Policies Cannot Be a Ground for Prosecution, 14 April 2020, https://aej-bulgaria.org/en/criticizing-anti-pandemic-measures-and-policies-cannot-be-a-ground-for-prosecution/

a person became guilty of the act, he was punished by imprisonment of up to three years, and in case of serious damage, by imprisonment of up to five years and fine of BGN 10,000 (approx. 5,100 EUR) to 50 000 (approx. 25,600 EUR)[19].

In March 2020, the parliamentary Culture and Media Commission rejected the proposal to amend the Radio and Television Act. The amendment proposed to attribute the Council for Electronic Media with the authority to announce that a certain website disseminates disinformation on the Internet and to ask a certain judicial authority to order that all providers and services of electronic communication networks discontinue accessing the website. The amendment also suggested defining disinformation in an internet environment as 'spreading on social networks, internet sites or in other ways in an internet environment through websites accessible on the territory of the Republic of Bulgaria, of a publication that contains false information that affects natural or legal persons'[20].

Another draft law, the proposals for amendments to the Personal Data Protection Act, was presented in May 2020. It proposed including the same definition of 'disinformation in the internet environment' as in the second proposal. The amendment proposes to assign responsibility for disinformation dissemination to the owners of websites, on-line platforms, social media accounts, and on-line blogs, as well as in certain cases domain providers, owners of on-line platforms, social networks, or blogs. It also gives powers to the Commission for Personal Data Protection to exercise control over the dissemination of disinformation[21].

3.2.4 Croatia

According to the research, Croatia belongs to the group of EU countries that ignore or deny the existence of Russian disinformation and hostile influence operations[22]. On the other hand, Croatia is one of the few countries that has removed the general crime of dissemination of false news from its Criminal Code in the evolution of regulation. Currently, the dissemination of false news is considered a misdemeanour in the Croatian legal system. Article 16 of the Law on Misdemeanours against Public Order and Peace punishes inventing or spreading false news that disturbs the peace and tranquillity of citizens. A fine or imprisonment of up to 30 days is envisaged for the prohibited act[23]. The consequence of this act is a disturbance of the peace and tranquillity of the citizens, so false news placed in public will not be considered a misdemeanour unless the consequence required by the legal description of the misdemeanour is caused[24].

There have been intentions to regulate and define accountability for content published online[25]. The Bill on Hate Speech adopted in June 2018 addressed the need to have the responsibility for hate

[19] Krusteva, Desislava, Makshutova, Radoslava. Bulgaria: Legislative attempts to restrict disinformation in 2020, OneTrust DataGuidance, August 2020: https://www.dataguidance.com/opinion/bulgaria-legislative-attempts-restrict
[20] Krusteva, Desislava, Makshutova, Radoslava. Bulgaria: Legislative attempts to restrict disinformation in 2020, OneTrust DataGuidance, August 2020: https://www.dataguidance.com/opinion/bulgaria-legislative-attempts-restrict
[21] Krusteva, Desislava, Makshutova, Radoslava. Bulgaria: Legislative attempts to restrict disinformation in 2020, OneTrust DataGuidance, August 2020: https://www.dataguidance.com/opinion/bulgaria-legislative-attempts-restrict
[22] Kremlin Watch Report, 16 May 2017, Overview of countermeasures by the EU28 to the Kremlin's subversion operations. How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies? P. 11, https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf
[23] Law on Misdemeanours against Public Order and Peace, https://www.zakon.hr/z/279/Zakon-o-prekr%C5%A1ajima-protiv-javnog-reda-i-mira,
[24] Pilić, M., Pilić, M. (2021) Infodemija u doba covida-19: kaznenopravni i sigurnosni aspekt. Polic. sigur. 3, https://hrcak.srce.hr/file/385061
[25] HINA, 'Most Croatian Media Without Fake News on Pandemic', 11 October 2020, https://www.total-croatia-news.com/news/47317-most-croatian-media-without-fake-news-on-pandemic

speech, public incitement to violence, and the spread of fake news in the Criminal Code[26]. However, by October 2020, no relevant legislative amendment was adopted[27].

As in other countries, the Criminal Code of Croatia establishes the criminal offence of false alarm. Article 316 of the Criminal Code prohibits falsely informing public services, ensuring order, or providing assistance of an event which requires urgent assistance by this service. The criminal act is punishable by imprisonment of up to three years[28]. Scholars note that the general criminal offence of spreading false news and alarming rumours was prescribed in the Criminal Code of 1997[29]. Article 322(1) of the Criminal Code prohibited the assertion, dissemination, or spreading of rumours that a person knew to be false with the aim of creating anxiety among a large number of citizens and where such anxiety really occurred[30]. However, during the reform of 2003, the general prohibition of spreading false and disturbing rumours was repealed, and the criminal offence which corresponds to the current criminal offence of false alarm was left in the Criminal Code[31].

3.2.5 Cyprus

The Cyprus Penal Code prohibits the acts of publicising any form of false news as a misdemeanour since 1962. Article 50 of the Code criminalised any false or potentially false statement, rumour or report, publication or reproduction of which will or is likely to cause fear or alarm to the public or intent to disturb the public peace[32].

The regulation currently in force includes a slightly modified description of potential harm. It goes beyond the disturbance of public order to diminish public confidence in the state's authorities or by causing fear or anxiety in the public or in any way disrupting the common peace and order. A person who is found guilty of the crime is punished with up to two years in prison or with a fine. The second paragraph of Article 50(1) of the Penal Code specifies that in case the publication was made in good faith or in circumstances justifying its publication, the act does not constitute a crime[33].

3.2.6 Czech Republic

The term ‘disinformation’ or ‘propaganda’ is not recognized legally in the Czech legal system; therefore, naturally relevant crimes are not defined[34]. As Filipec observes, legal protection is provided ‘against the most important effects of disinformation or misinformation, but does not address the real substance of disinformation or misinformation’[35].

One of the provisions embedded in the Czech Penal Code prohibits spreading alarming news. Section 357 of the Code criminalises intentional spreading of false alarming news that causes a threat of serious concern of at least a portion of the population of a certain area. The criminal act is

[26] Funke, D., Flamini, D. ‘A guide to anti-misinformation actions around the world. Croatia’, Poynter, https://www.poynter.org/ifcn/anti-misinformation-actions/#croatia
[27] HINA, ‘Most Croatian Media Without Fake News on Pandemic’, 11 October 2020, https://www.total-croatia-news.com/news/47317-most-croatian-media-without-fake-news-on-pandemic
[28] Croatian Criminal Code, https://www.legislationline.org/download/id/7896/file/Croatia_Criminal_Code_2011_en.pdf
[29] Croatian Criminal Code No. 110 of October 21, 1997, http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf
[30] Pilić, M., Pilić, M. (2021) Infodemija u doba covida-19: kaznenopravni i sigurnosni aspekt. Polic. sigur. 3, p. 423, https://hrcak.srce.hr/file/385061
[31] Pilić, M., Pilić, M. (2021) Infodemija u doba covida-19: kaznenopravni i sigurnosni aspekt. Polic. sigur. 3, p. 423, https://hrcak.srce.hr/file/385061
[32] Criminal Code of Cyprus of 1959, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=NIM:289553
[33] Criminal Code of Cyprus (text amended in 2021), http://www.cylaw.org/nomoi/enop/ind/0_154/section-sc538de4e7-f17f-4668-a2b7-34f90b34ac1e.html
[34] Filipec, O. (2019) Towards a Disinformation Resilient Society? The Experience of the Czech Republic, Cosmopolitan Civil Societies: an Interdisciplinary Journal, 11 (1), p. 10, https://doi.org/10.5130/ccs.v11.i1.6065
[35] Filipec, O. (2019) Towards a Disinformation Resilient Society? The Experience of the Czech Republic, Cosmopolitan Civil Societies: an Interdisciplinary Journal, 11 (1), p. 10, https://doi.org/10.5130/ccs.v11.i1.6065

punished by imprisonment for up to two years or by a prohibition of activity[36]. The aggravated form of the criminal act is established when the untrue news can cause precautions leading to a risk of serious concern of at least a portion of population of a certain place or an unfounded rescue operation of the integrated emergency system to public authorities, a legal person, a natural person who is an entrepreneur, or a mass communication media. In such a case, the punishment may increase to imprisonment of up to three years[37].

3.2.7 Denmark

In response to possible Russian influence campaigns[38] in 2018, Denmark's government adopted a plan of 11 initiatives to strengthen resilience[39], which included increased coordination of the authorities' efforts to identify and counteract influence operations, informing decision makers or the population that an influence operation is underway[40]. It also included a legislative proposal, which aims to criminalize influence campaigns launched by foreign intelligence services. The proposal presented in 2019 was approved by the Parliament by including Section 108 in the Criminal Code of Denmark and criminalising influence operations that may affect decision making or formation of public opinion[41]. Section 108 of the Code prohibits actions that assist or enable foreign intelligence services to act immediately or directly within the territory of the Danish state, including cooperation to carry out advocacy activities with a view to influence decision-making or public opinion formation. The criminal act is punishable by imprisonment for up to 6 years. The penalty may increase to 12 years' of imprisonment in the case of intelligence relating to military matters, or actions taking place during war or occupation, or if the influence campaign is exercised in connection with Danish national and EU parliamentary elections (in the framework of Section 116 of the Code).[42] The views on whether this provision covers comments and posts published on social media platforms differ[43]. Some scholars argue that it does not, since they are generally not considered a foreign power[44]. The use of bots in connection with prohibitions on foreign influence activities is not covered either, despite this issue being referenced in the amendment's draft bill on foreign interference[45].

Denmark also focuses on protecting the stability of the prices of securities, goods, real estate and other similar assets from the significant impact of misleading information. Sections 296 & 297 of the Criminal Code criminalise spreading false or misleading information, which can affect the price of above mentioned assets significantly. The crime is punished by a fine or imprisonment for up to one year and six months. The punishment may be reduced to a fine or, in aggravating circumstances,

[36] Criminal Code of the Czech Republic, https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf
[37] Criminal Code of the Czech Republic, https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf
[38] Proposals to Act amending the Criminal Code of Denmark (Illegal influence activities), https://www.ft.dk/ripdf/samling/20181/lovforslag/l95/20181_l95_som_fremsat.pdf
[39] Ministry of Foreign Affairs of Denmark, Strengthened safeguards against foreign influence on Danish elections and democracy, 7 September 2018, https://um.dk/en/news/newsdisplaypage/?newsid=1df5adbb-d1df-402b-b9ac-57fd4485ffa4
[40] Proposals to Act amending the Criminal Code of Denmark (Illegal influence activities), https://www.ft.dk/ripdf/samling/20181/lovforslag/l95/20181_l95_som_fremsat.pdf
[41] Act No. 269 amending the Penal Code of 26/03/2019, https://www.retsinformation.dk/eli/lta/2019/269
[42] The Criminal Code of Denmark, https://danskelove.dk/straffeloven
[43] Amnesty International, Høringsnotat, 11 October 2018 https://amnesty.dk/wp-content/uploads/media/5012/amnesty-international-hoeringssvar-om-hjaelp-til-fremmede-efterretningstjenester.pdf
[44] The Law Library of Congress, Global Legal Research Directorate, Government Responses to Disinformation on Social Media Platforms: Comparative Summary, https://www.hsdl.org/?view&did=835597
[45] The Law Library of Congress, Global Legal Research Directorate, Government Responses to Disinformation on Social Media Platforms: Comparative Summary, https://www.hsdl.org/?view&did=835597

imprisonment for any term not exceeding four months in case the above-mentioned acts have been committed through *gross* negligence[46].

3.2.8 Estonia

Estonia, being a highly digitalized country, faces the greater threat of having to face a technological intervention in democratic processes. However, despite a big concern regarding Russia's involvement through cyberattacks or organised disinformation campaigns, instead of relying on legislative action to address this issue, Estonia takes a non legislative approach[47].

The Estonian Penal Code criminalises false alarms in Article 278. However, the criminal act is constructed in narrow terms and prohibits only 'false emergency calls'[48]. Therefore, its application in the context of disinformation is irrelevant.

3.2.9 Finland

The Finnish government has recognized foreign disinformation as a genuine problem after Russia's annexation of Crimea in 2014; however, it has not specifically targeted disinformation through legal regulation[49]. The country *takes a non legislative approach* by taking soft measures such as educational programs, media literacy activities, task forces, monitoring, support of research, etc.

Similarly to Denmark, Finnish Criminal Code introduces a marketing offence for false or misleading information within specific market, however, this criminal act targets only marketing professionals in the field of goods, services, real estate, bonds, securities, or other commodities[50]. The Criminal Code also included the crime of false alarm; however, the criminal act is narrowed down to 'alarm about a bomb, fire, shipwreck, major accident, or other comparable distress or danger[51], therefore, it has no direct relevance to fighting disinformation.

3.2.10 France

France belongs to a small group of European countries which has a long-standing general prohibition of dissemination of fake news. Particular attention in the country is also paid to the protection of democratic processes, elections in particular.

Firstly, there is a general prohibition of the distribution of 'fake news' established in the Freedom of the Press Law since 1881. Article 27 of the law prohibits intentional publication, spreading, or reproduction, by any means of false news *('nouvelles fausses' in French*), the facts that are fabricated, falsified, or deceptively attributed to third parties, which have or could have disturbed public peace. The criminal delict is punished by a fine of 45,000 euros, or 135,000 euros fine if the

[46] The Criminal Code of Denmark, https://www.legislationline.org/download/id/6372/file/Denmark_Criminal_Code_am2005_en.pdf
[47] 'Tackling Disinformation and Online Hate Speech: Case studies of 27 EU Member States, so far', Democracy Reporting International, February 2021, p. 14, https://digitalmonitor.democracy-reporting.org/wp-content/uploads/2021/02/Tackling-Disinformation-and-Online-Hate-Speech-27-Case-Studies.pdf
[48] Article 278 of the Penal Code of Estonia, https://www.legislationline.org/download/id/9098/file/EST_CC_as%20of%20May%202021.pdf
[49] 'Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States: - 2021 update', April 2021, https://www.sipotra.it/wp-content/uploads/2021/05/Disinformation-and-propaganda-impact-on-the-functioning-of-the-rule-of-law-and-democratic-processes-in-the-EU-and-its-Member-States-2021-update.pdf
[50] Paragraph 1 of Chapter 30 'Trade offenses' of Finnish Criminal Code reads as follows, https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_19951010.pdf
[51] Paragraph 10 of Chapter 34 'Endangerment', https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_19951010.pdf

undesired act is likely to weaken the discipline or the morale of the army or to hinder the nation's war effort (Article 27(2) of the Law)[52].

Secondly, France criminalizes the distortion of the outcome of the election by 'false news'[53]. Article 97 of the Code, which content-wise has remained unmodified since 1964[54], envisages criminal responsibility of persons who with the help of false news, slanderous rumours or other fraudulent manoeuvres, surprised or deflected votes, determined one or more voters to abstain from voting. The delict is punishable with one-year imprisonment and a fine of 15,000 euros[55].

Law No. 2018–1202 on the fight against the manipulation of information[56] modified the Electoral Code. Article L. 163-2 empowers a judge to take all proportionate and necessary measures to stop the dissemination through an online public communication service of inaccurate or misleading allegations or imputations of a fact likely to alter the sincerity of the upcoming ballot that are disseminated deliberately, in a deliberate, artificial or automated and massive manner[57]. The court is obliged to decide within 48 hours from the referral, and the appeal decision is delivered in the same timeframe (Article L. 163-2(II)). The case may be initiated at the request of the public prosecutor, of any candidate, of any political party or group, or of any person having an interest in acting. The provision is applicable in the period that starts three months before the first day of the month of general elections and ends on the day of the ballot[58].

Furthermore, Article L. 163-1 imposes on the operators of the online platform during the same period transparency obligations relating to the promotion of 'information content related to a debate of general interest'. The operators of on-line platforms are required to disclose the identity of the persons who pay the platform remuneration in return for the promotion of such information and make public the amount of remuneration received in return for the promotion of such information content when their amount exceeds a determined threshold. Article L. 112 sanctions the disregard of these obligations. Any violation of the provisions of Article L. 163-1 is punishable by one year's imprisonment and a fine of 75,000 EUR[59].

Furthermore, the law on the fight against the manipulation of information modified the law No. 86-1067 of 30 September 1986 relating to the freedom of communication. Article 33-1 empowers the Superior Audio-visual Council (national audio-visual regulatory authority in France) to decide on the distribution of television or radio services controlled by a foreign state that involves a serious risk of, inter alia, threatening public order, needs of national defence, harming the fundamental interests of the nation, including the smooth functioning of its institutions. According to Article 33-1-1 of the law, the Superior Audio-visual Council can during the election campaigns period defined above suspend the distribution of a licensed broadcasting service of a broadcaster controlled by a foreign state or placed under the influence of the state which deliberately disseminates false information likely to alter the fairness of the ballot[60].

---

[52] Loi du 29 juillet 1881 sur la liberté de la presse, https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/,
[53] Hoboken, J., Fathaigh, Ó R. (2021). Regulating Disinformation in Europe: Implications for Speech and Privacy, 6 UC Irvine Journal of International, Transnational, and Comparative Law, 9, https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1041&context=ucijil, p. 18.
[54] Décret n° 64-1086 du 27 octobre 1964 portant révision du code électoral, https://www.legifrance.gouv.fr/download/securePrint?token=@ZXug0XOZQC!6dScf4z$
[55] Code électoral, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000006148461/?anchor=LEGIARTI000006353232#LEGIARTI000006353232
[56] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/
[57] Regulating Freedom of Speech on Social Media: Comparing the EU and US Approach, https://law.stanford.edu/wp-content/uploads/2021/02/weiss_wp73.pdf
[58] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/
[59] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/
[60] Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/

In the wake of the adoption of the law by the National Assembly, the prime minister and more than 60 senators, including some from the presidential majority, appealed to the Constitutional Council, claiming that Article 1 and the new emergency procedure unnecessarily, inappropriately, and disproportionately contravened the freedom of expression and communication[61]. They also argued that the newly created offence of infringing the new transparency obligations of online platforms violated the constitutional principle of the legality of offences and penalties[62].

On the initiative of the Prime Minister and more than 60 senators, the law on the fight against the manipulation of information was brought before the Constitutional Council for the constitutionality assessment[63]. In its decision No. 2018-773 of 20 December 2018, the Constitutional Council of France found the newly adopted provisions consistent with the Constitution. Regarding transparency obligations under Article 163-1, in paragraphs 8 & 9 of the decision the Council observed that these duties are temporary in nature and content wise since the information content relating to a debate of general interest covered by the contested provisions is that which has a link with the electoral campaign. Additionally, in the view of the Council, the provision aims to provide citizens with the means to assess the value or the scope of the information thus promoted and thereby contributing to the clarity of the electoral debate[64]. Thus, given the purpose of the general interest pursued and the limited nature of the obligation imposed on online platform operators, the contested provisions do not disproportionately affect the freedom to conduct business[65]. As for Article L. 163-2, the Council paid attention that by introducing the provision, the legislator intended to ensure the clarity of the electoral debate and respect for the principle of sincerity of the ballot (para. 18). In addition to the temporary and content-wise restricted nature of the provision, the Council observed that the summary procedure only concerns public content published on online communication services that lend themselves more easily to massive and coordinated manipulations because of their multiplicity and the particular methods of distribution of their content[66]. Furthermore, the Council emphasised that the legislature has strictly delimited the information which may be the subject of the contested summary proceedings. Only the dissemination of such allegations or accusations that meet three cumulative conditions can be called into question: they must be artificial, automated, massive, and deliberate. These allegations or imputations do not cover opinions, parodies, partial inaccuracies, or mere exaggerations. They are those whose falsity can be objectively demonstrated[67].

3.2.11 Germany

In 2017, in response to the lack of self-regulatory efforts of social media platforms to a peak of hate speech and disinformation on social media stimulated by the flow of Syrian asylum seekers to the country in 2015 platforms[68], Germany passed the Act to Improve Enforcement of the Law in Social

[61] IRIS newsletter, https://merlin.obs.coe.int/newsletter/download/241/pdf/E
[62] Laws to Combat Manipulation of Information Finally Adopted, https://merlin.obs.coe.int/article/8446
[63] Blocman, A. 'Laws to combat manipulation of information finally adopted', European Audiovisual Observatory, https://merlin.obs.coe.int/article/8446
[64] Decision no. 2018-773 DC of 20 December 2018, https://www.conseil-constitutionnel.fr/en/decision/2018/2018773DC.htm
[65] Paragraphs 8, 9, Décision n° 2018-773 DC du 20 décembre 2018, https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm#:~:text=LE%20CONSEIL%20CONSTITUTIONNEL%20A%20%C3%89T%C3%89,21%20novembre%202018%2C%20par%20MM.
[66] Paragraphs 18-20, Décision n° 2018-773 DC du 20 décembre 2018, https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm#:~:text=LE%20CONSEIL%20CONSTITUTIONNEL%20A%20%C3%89T%C3%89,21%20novembre%202018%2C%20par%20MM.
[67] Paragraphs 21, Décision n° 2018-773 DC du 20 décembre 2018, https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm#:~:text=LE%20CONSEIL%20CONSTITUTIONNEL%20A%20%C3%89T%C3%89,21%20novembre%202018%2C%20par%20MM.
[68] Heldt, A. 'Germany is amending its online speech act NetzDG... but not only that', Internet Policy Review, https://policyreview.info/articles/news/germany-amending-its-online-speech-act-netzdg-not-only/1464

Networks (Netzwerkdurchsetzungsgesetz, NetzDG)[69] (also called the 'Facebook Act')[70]. The law did not create any new duties for social media platforms, but did impose high fines for non-compliance with existing legal obligations[71].

Section 1 of the Network Enforcement Act describes the scope of its application. Under Section 1(1), firstly, the act is applicable to social networks, i.e., tele media service providers which, for profit-making purposes, operate internet platforms designed for sharing any content among users or making it public; secondly, only those social networks that have 2 million or more registered users in Germany are triggered by the law (Section 1 (2))[72].

The Act obliges social network providers, as defined above, to provide users with an easily recognisable, directly accessible, and permanently available procedure to submit complaints about unlawful content and to maintain an effective and transparent procedure for their handling (Section 2 (1)). The provider must remove or block access to 'manifestly unlawful' content within 24 hours after receiving the complaint (Section 3(2(2))). In case the unlawfulness is not manifest, the obligation to remove or block access to all unlawful content must meet the limit of 7 days. If the decision on the unlawfulness of the content is dependent on the falsity of a factual allegation or is clearly dependent on other factual circumstances, the social network can give the user the opportunity to respond to the complaint before making the decision. In this case, the 7-day time limit may be exceeded. The extension of the time limit is also possible if the social network refers the decision regarding unlawfulness to a recognised self-regulation institution within 7 days of receiving the complaint and agrees to accept the decision of that institution (Section 3 (2(3)))[73]. A social network may be fined up to 50 million euros.

It is essential that the unlawful content reaches the threshold of certain offences under the German Criminal Code (Section 1(3)). The Network Enforcement Act provides a list of unlawful activities that fall within the scope of application of this Act. Only a few of them include offences relevant to disinformation (in particular under the title 'Endangering democratic state under rule of law'), although, indirectly, since the German criminal code does not prohibit disinformation per se. Section 145 of the Criminal Code prohibits the misuse of emergency numbers and the alteration of means of accident prevention and first aid[74]. However, the norm is defined in narrow and specific terms and does not leave the space for incorporation of any disinformation related activities.

The Network Enforcement Act has been criticised as unconstitutional and infringing on freedom of speech. The critics suggested that given these costs as well as tight deadlines and heavy fines, platforms would have a strong incentive simply to comply with most complaints, thus encouraging the removal of legal content. A judicial authority is not included in takedown decision making, there is no clear appeals handling mechanism for victims to seek independent redress either[75].

[69] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=433744569E4AA4A03CED91951420A4DA.2_cid297?__blob=publicationFile&v=2

[70] Library of Congress, 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech', https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

[71] Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech, https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

[72] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=433744569E4AA4A03CED91951420A4DA.2_cid297?__blob=publicationFile&v=2

[73] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=433744569E4AA4A03CED91951420A4DA.2_cid297?__blob=publicationFile&v=2

[74] German Criminal Code, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1441

[75] Tworek, H., Leerssen, P. An Analysis of Germany's NetzDG Law, 15 April 2019, https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

3.2.12 Greece

Greece criminalized 'false news' with a reform of the penal code in March 2019 in Chapter 6 of 'Crimes Against Public Order.' Article 191 (1) of the Greek Penal Code sanctioned a person with imprisonment of up to 3 years or a fine for 'dissemination of false news' that results in fear of an indefinite number of people or damage to the country's economy, tourism, defence and bilateral relationship. If a person becomes guilty of the act negligently, s/he may be fined or punished by the provision of community service (Article 191 (2) of the Penal Code)[76].

The need to tackle misinformation during the pandemic resulted in the proposal brought forward by the Ministry of Justice to amend Article 191 of the Greek Penal Code, which found its way to the Parliament and was approved in November 2021. The new provision modifies the definition of possible harm: 'causing concern or fear in the public or affecting public confidence in the national economy, the defence capacity of the country, or public health'[77]. The modification also adds the element of repetition of a prohibited conduct. If the spread is repeated through the press or online, the minimum sentence increases to six months of imprisonment and a fine. These penalties are not limited to the person who is the source of the information. They also apply to the owners and directors of the media that publish it, or simply publish links to it[78]. The offence defined in Article 191 of the Penal Code is categorised as a misdemeanour, which under Greek law is punishable with imprisonment of a maximum of five years[79].

The proposal was criticised for leaving open door to censorship of legitimate reporting and creating, and additional avenue for journalists to face prosecution and jail time[80]. Critics paid attention to the absence of definition or criteria to determine what fake news is or its link in the legal provision to any actual harm[81].

3.2.13 Hungary

The crime of scaremongering was introduced into the Hungarian Criminal Code in 2001. The revised Criminal Code of 2012 left the wording of the criminal act established in Section 337 unchanged[82]. Section 337 prohibited any conduct of claiming or spreading a knowingly false or distorted fact before a large public. Furthermore, the provision required that the conduct be 'suitable to alarm or agitate a large group of people at the site of a public emergency'[83]. In Hungarian criminal law, 'public emergency' means an 'objective situation where one or more undefined or numerous defined people, or things of higher value can be in danger' (BH1998. 304)[84]. The phrase 'at the site' implies that the public emergency must be geographically and temporally localised and that false statements can

[76] Article 191 of Greek Penal Code, https://collab.lawspot.gr/sites/default/files/mashup/feka/2021/fek-215-2021.pdf
[77] Amendments to the Penal Code, the Code of Criminal Procedure and other provisions, https://collab.lawspot.gr/sites/default/files/mashup/feka/2021/fek-215-2021.pdf
[78] Reporters without borders, New Greek law against disinformation endangers press freedom, https://rsf.org/en/news/new-greek-law-against-disinformation-endangers-press-freedom,
[79] Based on the gravity and certain circumstances under which the crimes have been committed the crimes are divided into misdemeanors and felonies in the new Greek Penal Code. Labadarios Law Firm, https://www.lambadarioslaw.gr/2019/07/new-criminal-code-and-new-code-of-criminal-proceedings-to-come-into-force-as-of-01-07-2019-in-greece/
[80] European Centre for Press and Media Freedom, Greece: Justice Ministry must withdraw amendment on 'false news', 12 October 2021, https://www.ecpmf.eu/greece-justice-ministry-must-withdraw-amendment-on-false-news/
[81] Human Rights Watch, 'Greece: Alleged 'Fake News' Made a Crime', https://www.hrw.org/news/2021/11/17/greece-alleged-fake-news-made-crime,
[82] Győry, Csaba, *'Fighting Fake News or Fighting Inconvenient Truths?: On the Amended Hungarian Crime of Scaremongering', VerfBlog,* 2020/4/11, https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/, DOI: 10.17176/20200411-152518-0.
[83] Act C of 2012 on the Criminal Code, promulgated on 13 July 2012, https://www.legislationline.org/download/id/5619/file/HUngary_Criminal_Code_of_2012_en.pdf
[84] https://www.ecpmf.eu/wp-content/uploads/2020/06/Legal-opinion-Hungary_2020.pdf

disturb people in the physical location[85]. The felony offence is punished by imprisonment of up to three years[86]. So far, there has been almost no case law related to the crime of scaremongering in Hungary[87].

In contrast to other countries, Hungarian criminal law does not contain a narrowly structured prohibition of false alarm. Instead, it criminalizes the threat of public endangerment, which covers statements or the dissemination of 'any untrue fact intended to disturb public peace' or giving 'the impression that there is imminent danger of the occurrence of an event that is likely to cause harm to the general public'. The felony offence established in Section 338 of its Criminal Code is punished by imprisonment between one and five years if the threat of public endangerment has resulted in a grave disturbance of public peace[88].

Recent studies present Hungary as a country that largely ignores and denies Russia's disinformation and hampers civil society in countering Russia's influence[89]. Not surprisingly, in terms of disinformation, the country's legislative landscape has not changed over the years. In response to the COVID-19 'infodemic', the Anti-Coronavirus Act No. 12 of 2020 amended Section 337 of the Criminal Code[90]. As observed by Győry, the first change introduced in the amendment was related to the specification that falsehood or distorted fact must be related to public emergency. The second major change is related to the appearance of the aggravated form of the offence[91]. The aggravated form covers the actions taken while the special legal order is in force regardless of the location. Additionally, it must be an action hindering the success of the state defence against the danger that led to the introduction of the special legal order[92].

The Hungarian Constitutional Court concluded on June 17, 2020, that the new criminal provision is constitutional. The Constitutional Court ruled that the disputed regulation only applies to a limited set of communications. The prohibition applies only to statements of fact that are knowingly false or distorted, not to critical viewpoints. The legislation, according to the Court, does not apply to communications in which the perpetrator was not informed that the information contained in the communication was incorrect[93].

3.2.14 Ireland

In early December 2017, the proposal for the Online Advertising and Social Media (Transparency) Bill was introduced that would criminalise the use of a bot to cause multiple online presences directed towards a political end to present as an individual account or profile on an online platform made using a bot to spread political messages. According to the bill, using a bot to create 25 or more

---

[85] Győry, C. (2020) *Fighting Fake News or Fighting Inconvenient Truths?: On the Amended Hungarian Crime of Scaremongering, VerfBlog,* 2020/4/11, https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/, DOI: 10.17176/20200411-152518-0.

[86] Act C of 2012 on the Criminal Code, promulgated on 13 July 2012, https://www.legislationline.org/download/id/5619/file/HUngary_Criminal_Code_of_2012_en.pdf

[87] Polyák Gábor, Mertek, Hungary's Two Pandemics: COVID-19 and Attacks on Media Freedom, European Centre for Press and Media Freedom, 2020, https://www.ecpmf.eu/wp-content/uploads/2020/06/Legal-opinion-Hungary_2020.pdf

[88] Act C of 2012 on the Criminal Code, promulgated on 13 July 2012, https://www.legislationline.org/download/id/5619/file/HUngary_Criminal_Code_of_2012_en.pdf

[89] Kremlin Watch Report, 16 May 2017, Overview of countermeasures by the EU28 to the Kremlin's subversion operations. How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies?
https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf

[90] Text of the anti-coronavirus act in Hungarian available here: https://magyarkozlony.hu/dokumentumok/9b48945c85f190378f67e253337be4299edf743f/megtekintes

[91] Győry, Csaba, *Fighting Fake News or Fighting Inconvenient Truths?: On the Amended Hungarian Crime of Scaremongering, VerfBlog,* 2020/4/11, https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/, DOI: 10.17176/20200411-152518-0.

[92] Győry, Csaba: *Fighting Fake News or Fighting Inconvenient Truths?: On the Amended Hungarian Crime of Scaremongering, VerfBlog,* 2020/4/11, https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/, DOI: 10.17176/20200411-152518-0.

[93] ECPMF, 'Hungary's two pandemics: COVID-19 and attacks on media freedom', 17 June 2020, https://www.ecpmf.eu/hungarys-two-pandemics-covid-19-and-attacks-on-media-freedom/

personas on social media would be punishable by up to five years in prison or fines of up to 1000 Euro[94]. The proposal was rejected by the Chamber of Deputies[95].

By 31 March 2021, the discussions on the Bill were restored before the Chamber of Deputies[96]. The bill provides for stronger scrutiny of online political advertising related to elections and new transparency obligations such as the data of payer of the ad, why the person was targeted, and the cost of running the ad itself[97]. Social media representatives argued that the proposed changes could have a negative impact on privacy and contradict the legal framework of the European Union on online political advertising[98]. On 30 November 2021, the proposed regulation was not yet adopted.

3.2.15 Italy

Like in some other countries, Italian criminal law provisions prohibit the publication and dissemination of news that disturbs public order[99]. Article 656 of the Italian Criminal Code does not use the term disinformation or fake news. Instead, the criminal act is associated with publication and dissemination of *false, exaggerated or biased news*[100]*.* News is defined in the law as an announcement or information whose content is precise and recognizable, excluding generic, vague statements or statements referable to rumours[101]. According to the practice of the Supreme Court, the fact that no disturbance of public order occurred is not relevant to establishing the fact that the criminal act was committed. It suffices to show that there was an abstract possibility that such a disturbance would occur[102].

The criminal act is regarded as misdemeanour, since the committing of the criminal act may be punished by arrest for up to three months or with a fine of up to 309 Eur. The rising anti-establishment Five Star Movement, which proliferated disinformation and pro-Kremlin propaganda during the constitutional referendum in December 2016, raised first concerns about disinformation and hostile influence operations in Italy[103]. In 2017, a proposal to amend Article 656 of the Criminal Code was presented to the Italian Parliament. It was suggested to introduce a stricter penalty from three months to five years of imprisonment and reformulate the provision by explicitly including the use of the telephone network or through telematics or IT tools and unjust damage to people as a possible damage. The penalty is increased if the offense is committed for profit or if the news relates to acts

[94] Online Advertising and Social Media (Transparence) Bill 2017, https://web.archive.org/web/20180506190500/http://www.oireachtas.ie/documents/bills28/bills/2017/15017/b15017d.pdf,
[95] O'Halloran, M., 'Government defeated on online advertising and social media Bill', 14 December 2017, https://www.irishtimes.com/news/politics/oireachtas/government-defeated-on-online-advertising-and-social-media-bill-1.3327979
[96] Online Advertising and Social Media (Transparency) Bill 2017: Restoration to Order Paper, https://www.oireachtas.ie/en/debates/debate/dail/2021-03-31/16/
[97] Stolton, Samuel, 'Facebook urges Ireland to hold off on political ads rules until EU legislation', Euractiv, Mar 30, 2021, https://www.euractiv.com/section/digital/news/facebook-urges-ireland-to-hold-off-on-political-ads-rules-until-eu-legislation/
[98] Stolton, Samuel, 'Facebook urges Ireland to hold off on political ads rules until EU legislation', Euractiv, Mar 30, 2021, https://www.euractiv.com/section/digital/news/facebook-urges-ireland-to-hold-off-on-political-ads-rules-until-eu-legislation/
[99] Article 656 of the Italian Criminal Code reads as follows: "Anyone who publishes or disseminates false, exaggerated or biased information (1), for which public order may be disturbed, is punished, if the fact does not constitute a more serious crime [265, 269, 501, 658] (2), with imprisonment for up to three months or with a fine of up to 309 Eur".
[100] Brocardi.it, https://www.brocardi.it/codice-penale/libro-terzo/titolo-i/capo-i/sezione-i/art656.html
[101] Brocardi.it, https://www.brocardi.it/codice-penale/libro-terzo/titolo-i/capo-i/sezione-i/art656.html
[102] Cassazione penale, Sez. I, sentenza n. 9475 del 7 novembre 1996
[103] Kremlin Watch Report, 16 May 2017, Overview of countermeasures by the EU28 to the Kremlin's subversion operations. How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies?
https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf

of violence of a racial, sexual, or otherwise discriminatory nature[104]. However, 'such a proposal was considered repressive and likely to cause widespread forms of censorship'[105].

In January 2018, before the general elections, the Italian Interior Ministry enacted the 'Operating Protocol for the Fight Against the Diffusion of Fake News through the Web on the Occasion of the Election Campaign for the 2018 Political Elections'[106]. The protocol empowered the Postal Police autonomously or by following people's reports of hoaxes through a dedicated portal to check the news and report if the content is unlawful (defamatory) to the judicial authority[107]. In cases where false or misleading content was established, but not unlawful content, public denials were published[108].

The document was widely criticised by human rights activists for the excessive discretionary power of the police[109]. Special Rapporteur on the promotion and protection of the right to freedom of opinion D. Kaye requested to abolish the Protocol, since it included 'general prohibitions on the dissemination of information based on vague and ambiguous ideas, including 'false news' or 'non-objective information', thus infringing freedom of expression[110].

The false identity issue, particularly relevant in the context of disinformation[111], has been indirectly addressed in Italian case law in the context of misinformation. On 28 July 2018, in its decision no. 1680 an Italian criminal court in Lecce sentenced a TripAdvisor reviewer for fraudulent reviews to imprisonment of nine months[112]. The person was charged with fraud and impersonation crimes. Article 494 of the Italian Criminal Code[113] criminalises stealing or using someone's identity for personal benefits or causing damage[114]. Social media representatives called this ruling a landmark decision, as it was the first time a person faced criminal responsibility for selling fake news.

3.2.16 Latvia

On 30 November 2021, no legislative measures had been adopted in the country that would directly target disinformation. The country *takes a non legislative approach* by taking soft measures such as educational programs, media literacy activities, task forces, monitoring, support of research, etc.

Latvia is the only Baltic state that applied existing criminal law provisions to fight false information. The National Police Cybercrime Unit launched a criminal investigation in July 2018 after several companies complained about the spread of fake online news about all kinds of disasters, road accidents, collapsed shopping mall, an airplane crash, etc.[115]. A person was found guilty of

[104] Camera dei Deputati, Modifica dell'articolo 656 del codice penale e altre disposizioni in materia di pubblicazione o diffusione di notizie false, esagerate o tendenziose, presentata il 15 giugno 2017, https://www.camera.it/leg17/995?sezione=documenti&tipoDoc=lavori_testo_pdl&idLegislatura=17&codice=17PDL0053180
[105] Sofia V., 'Tackling fake news, the Italian way', Resource Center on Media Freedom in Europe, 29 May 2018, https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way,
[106] Sofia V., 'Tackling fake news, the Italian way', Resource Center on Media Freedom in Europe, 29 May 2018, https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way,
[107] Sofia V., 'Tackling fake news, the Italian way', Resource Centre on Media Freedom in Europe, 29 May 2018, https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way,
[108] Reference of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL ITA 1/2018, 20 March 2018, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf,
[109] Sofia V., 'Tackling fake news, the Italian way', Resource Centre on Media Freedom in Europe, 29 May 2018, https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way,
[110] Reference of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL ITA 1/2018, 20 March 2018, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf,
[111] Ireton, C., Posetti, J., 'Journalism, fake news & disinformation: handbook for journalism education and training', https://unesdoc.unesco.org/ark:/48223/pf0000265552, p. 18.
[112] Funke, D., and Flamini, D., 'A guide to anti-misinformation actions around the world', Poynter, https://www.poynter.org/ifcn/anti-misinformation-actions/
[113] Changes of the law, https://www.lexology.com/library/detail.aspx?g=a2b6a2dd-f23a-43fe-a190-87177e5f66e3
[114] Criminal Code of Italy, https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-penale
[115] eng.lsm.lv, 'Man charged with hooliganism for running fake Latvian news websites', 16 July 2019, https://eng.lsm.lv/article/society/crime/man-charged-with-hooliganism-for-running-fake-latvian-news-websites.a325793/,

hooliganism and incitement to hatred on social media[116]. The police said that false information destabilised society and disrupted the operations of relevant agencies and businesses[117].

3.2.17 Lithuania

Disinformation is described in paragraph 4 of Article 25 of the Constitution as a criminal act incompatible with the freedom to express beliefs and disseminate information. Article 25 of the Constitution, inter alia, provides that freedom to express convictions and impart information is incompatible with the criminal actions of instigation of national, racial, religious, or social hatred, violence, discrimination, slander and disinformation. In its interpretation of this constitutional provision, the Constitutional Court of the Republic of Lithuania noted back in 2005 that the prohibition on disseminating information of the said content is absolute and draws attention to the duty of the legislator to establish the legal regulation that disinformation would be prosecuted as criminal actions and legal liability would be established for it as criminal actions[118]. It has been done by several criminal code provisions but never by an explicit criminalization of disinformation as defined by Lithuania's Law on the Provision of Information to the Public.

Paragraph 2 of Article 19 of the Law on Public Information of the Republic of Lithuania prohibits disinformation and for a long time Lithuania was the only EU Member State that had a statutory definition of 'disinformation'[119] (see: Portugal). Article 2(15) of the law defines the term as 'deliberately disseminating false information to the public'[120]. Therefore, to establish a breach of the obligation laid down in Paragraph 2 of Article 19, it is necessary to establish that the information disseminated is incorrect and deliberately disseminated.

It should be noted that the law underwent a revision at the beginning of 2021 and certain significant changes regarding legal liability for the act of disinformation were introduced. Before the amendment, the sanctions could be applied only in some cases specified in the law, e.g., in the cases where disinformation defamed, insulted a person, degraded his or her honour and dignity, the existence of acts such as calls for violation of the sovereignty of the Republic of Lithuania, independence or integrity of the territory, propaganda of war, incitement to war. The fines provided in the law were not applicable if only misinformation had been established. The amended law puts disinformation on the same footage as war propaganda, incitement to war, violent violation of the sovereignty of the Republic of Lithuania – change of its constitutional order, encroachment on its independence, or violation of the integrity of the territory, however, only in terms of legal effects envisaged in the law (Article 48 and Section VI).

The amendments had no effect on criminalising disinformation as defined by the law. The issue of criminalising disinformation has already been the subject of public debate a number of times. The proposal encouraged the addition to the Criminal Code with the provision establishing the liability for public incitement to violate Lithuania's sovereignty by disseminating false information to harm the national interests of the Republic of Lithuania or destabilize the state. It was regarded disproportionate given the broad language of the motive for the act. The opponents of the initiative paid attention to the fact that criminal liability in a democratic society had to be seen as the ultimate ratio used to protect the values in cases where less stringent measures cannot achieve the same goals, i.e., only when other sanctions were insufficient and ineffective. In this regard, the practice of the Constitutional Court of the Republic of Lithuania was taken into consideration, emphasising that

[116] 'Who calls the shots on fake news? The minefield of countering lies in the Baltics', lrt.lt, 29 May 2021, https://www.lrt.lt/en/news-in-english/19/1418424/who-calls-the-shots-on-fake-news-the-minefield-of-countering-lies-in-the-baltics
[117] 'Who calls the shots on fake news? The minefield of countering lies in the Baltics', lrt.lt, 29 May 2021, https://www.lrt.lt/en/news-in-english/19/1418424/who-calls-the-shots-on-fake-news-the-minefield-of-countering-lies-in-the-baltics
[118] The ruling of the Constitutional Court of Lithuania of 19 September 2005 'On the procedure for the dissemination of information not to be divulged to the public', https://www.lrkt.lt/en/court-acts/search/170/ta1309/content
[119] ERGA, 'Notions of disinformation and related concepts, 2021, p. 10 https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf
[120] Lietuvos Respublikos visuomenės informavimo įstatymas, https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr

there must be a strict balance between objectives and legal measures, which must not restrict the rights of the individual more than is necessary to achieve these objectives[121].

3.2.18 Luxembourg

On 30 November 2021, no legislative measures were adopted in the country that would be directly relevant to counter disinformation. The country *takes a non legislative approach* by taking soft measures such as educational programs, media literacy activities, task forces, monitoring, support of research, etc.

3.2.19 Malta

The Criminal Code of Malta specifically addresses the spread of false news. Article 82 of the Criminal Code criminalises 'the malicious spread of false news that is likely to alarm public opinion, disturb public order or peace, create a commotion among the public or among certain classes of the public'[122].

3.2.20 The Netherlands

On 30 November 2021, no legislative measures were adopted in the country that would be directly relevant to counter disinformation. The country *takes a non legislative approach* by taking soft measures such as educational programs, media literacy activities, task forces, monitoring, support of research, etc.

The Dutch Criminal Code criminalises false alarms in Section 142[123]. Intentional disturbance of peace by false cries or false signals is punishable with imprisonment of up to one year or a fine of the fourth category. There is no information that there was any intention to apply this provision in the context of disinformation. The criminal act in the second paragraph of Section 142 is constructed in narrow terms and prohibits only intentional use of an emergency number for public services[124]. Therefore, its application in the context of disinformation is irrelevant.

3.2.21 Poland

Poland focuses specifically on a fair election process. The 2011 Polish Election Code gives the power to intervene in the event that 'untrue data or information' about an election candidate is disseminated. The complaint must be heard by the judiciary authority within 24 hours (Article 111 (2) of the Code). According to paragraph 1 of Article 111 of the Code, the national court may prohibit the dissemination of above-mentioned information, confiscate the election material containing such information, order to rectify it, to publish the answers to statements which violate personal rights or apologise the person whose personal rights have been violated, and require the participant to the proceedings to pay the amount to 100,000 zlotys to an organisation of public benefit. The law requires the publication of the correction, reply, or an apology to take place at the latest within 48 hours, at the expense of the person ordered to do so (Article 111 (4) of the Code).

[121] The rulings of the Constitutional Court of Lithuania of 13 December 2004, 29 December 2004, 29 September 2005.
[122] Criminal Code of Malta, https://justice.gov.mt/en/pcac/Documents/Criminal%20code.pdf
[123] Section 142 of the Criminal Code of Netherlands,
[124] The Criminal Code of the Netherlands,
https://www.ejtn.eu/PageFiles/6533/2014%20seminars/Omsenie/WetboekvanStrafrecht_ENG_PV.pdf

On 30 November 2021, no other legislative measures have been adopted in Poland that would be directly relevant to countering disinformation.

3.2.22 Portugal

On 17 May 2021, the Portuguese national assembly approved the Portuguese Charter on Human Rights in the Digital Age[125]. Article 6 of the Charter establishes the right to protection against disinformation. Disinformation is defined in paragraph 2 of Article 6 as any narrative that is proven to be false or misleading, presented and disseminated to obtain economic advantage or to deliberately mislead the public, and which is likely to cause public harm, namely a threat to democratic political or public policy-making processes and public good. Article 6 clarifies that the use of manipulated or manufactured texts or videos, as well as practices to flood electronic mailboxes and the use of networks of fictitious followers, is considered to be, inter alia, demonstrably false or misleading information. Paragraph 4 of the same article excludes mere errors in the communication of information, as well as satires or parodies, from the definition of disinformation.

The law gives the power to the Regulatory Authority for the Media to assess complaints against any person that carries out the acts defined as disinformation and apply the sanctioning regime. The regulation granting the Authority the power to decide what is or is not legitimate content provoked the criticism of the Union of Journalists of Portugal, which found unacceptable the creation of a concept of 'disinformation' with legal consequences[126]. The review of constitutionality of the provisions of Article 6 of the Charter initiated by the President of Portugal on 28 July 2021 will clarify whether the legal regulation restricts the right to freedom of expression proportionally in line with Article 37 of the Constitution of the Portuguese Republic[127].

Paragraph 6 of Article 6 also establishes the State's support for the creation of structures for the verification of facts in properly registered media and encourages the attribution of quality seals by trustworthy entities endowed with the status of public utility. The Constitutional Court of Portugal will answer if this provision is in line of the Constitution of the Portuguese Republic since it foresees the State's action in the creation of structures for verification of facts whose scope of action is allegedly unknown[128].

As of 30 November 2021, no other legislative measures have been adopted in the country that would be directly relevant to countering disinformation.

3.2.23 Romania

Article 404 of the Romanian criminal code criminalises communication or dissemination, by any means of false news, data or information or of falsified documents, knowing their false character, if this endangers the national security[129]. From the perspective of the subjective side of the deed, the provision imposes the requirement that the perpetrator is aware of the false character of the news. The lack of this constitutive element leads to the non-existence of the crime[130]. The criminal act is

[125] Law No. 27/2021, Carta Portuguesa de Direitos Humanos na Era Digital, https://dre.pt/dre/detalhe/lei/27-2021-163442504

[126] 'SJ questiona constitucionalidade do artigo 6.º da carta dos direitos digitais', Sindicato dos Jornalistas, 9 June 2021, https://jornalistas.eu/sj-questiona-constitucionalidade-do-artigo-6-o-da-carta-dos-direitos-digitais/

[127] 'Article 6 of the Portuguese Charter on Human Rights in the Digital Age', Application send to the Constitutional Court, Presidency of the Portuguese Republic, https://www.presidencia.pt/atualidade/toda-a-atualidade/2021/07/artigo-sexto-da-carta-portuguesa-dos-direitos-humanos-na-era-digital/

[128] Presidency of the Portuguese Republic, Article 6 of the Portuguese Charter on Human Rights in the Digital Age, Application send to the Constitutional Court, https://www.presidencia.pt/atualidade/toda-a-atualidade/2021/07/artigo-sexto-da-carta-portuguesa-dos-direitos-humanos-na-era-digital/

[129] Indaco lege, https://lege5.ro/gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=ggytsojwge3te

[130] Indaco lege, https://lege5.ro/gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=ggytsojwge3te,

punishable with imprisonment from 1 to 5 years[131]. This crime was introduced in 2009; however, it was not new to Romania's legal landscape – the text was taken from Article 1681 of the Criminal Code of 1969. Two differences were introduced in the provision. The notion of 'state security' was replaced by 'national security' and the requirement to know the falsity of news, data, information or documents communicated or disseminated[132].

Article 404 of the Romanian criminal code was at the centre of legal discussions in fighting Covid-19 infodemia in 2020[133]. The issue in applying the provision to established cases of false information about coronavirus was that in most of the cases the users of a social network passing on the information were not aware of their falsity. In the absence of this knowledge, Article 404 could not be applied[134].

The declaration of a state of emergency in Romania to combat coronavirus brought about new legal measures related to media control. The decree of the President of Romania allowed the National Authority for Management and Regulation in Communication to order the removal of and blocking access to online content that "promotes false news" related to the measure for protection and prevention of COVID-19[135], resulting in the closing of the authorities that have started to close news sites[136]. The issue of this decree was the absence of any remedy available nor appeal[137].

3.2.24 Slovakia

Slovakia does not have any specific regulation targeting disinformation. As in most countries, Slovakia also criminalizes the dissemination of a false alarming message capable of causing danger to the public. According to Article 361 (1) of the Slovakian Penal Code adopted in 2005, the danger must be serious and must impact at least a part of the population in some area. The act is punishable by imprisonment for up to two years[138].

The aggravated form of the crime, which calls for 1 to 5 years of imprisonment, covers reporting a false alarming news, inter alia, to the mass media. However, to incriminate this prohibited action proving that a person knew that such news was false and might cause serious concerns among the population of a certain areas or at least in the parts of certain areas, is required[139]. The crime may be even punished three to eight years of imprisonment if the offence is repetitive or it significantly affect economic operations or economic activities of a legal entity or the activities of governmental authorities or raises other particularly serious consequence[140].

---

[131] Indaco lege, https://lege5.ro/gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=gqytsojwge3te,

[132] Indaco lege, https://lege5.ro/gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=gqytsojwge3te,

[133] Grosseck, G., Malita, L. (2020). Insights from Romania's Reaction to Coronavirus Infodemic. towardsan Educational Approach. Logos Universality Mentality Education Novelty: Social Sciences, 9(1), 119-138. doi: 10.18662/lumenss/9.1/38, https://lumenpublishing.com/journals/index.php/lumenss/article/view/3136/pdf, p. 128.

[134] Țară în service, Dezinformare și siguranță națională - cum amenință știrile false să destabilizeze România, https://romania.europalibera.org/a/31566084.html,

[135] Decree on the extension of the state of emergency in the territory of Romani, https://rm.coe.int/16809e375e,

[136] Gotev, G. Rotaru, S. 'Romania shuts down websites with fake COVID-19 news', https://www.euractiv.com/section/all/short_news/romania-shuts-down-websites-with-fake-covid-19-news/,

[137] BalkanInsight, Romania's State of Emergency Raises Media Freedom Concerns, by Marcel Gascon Barbera, 31st March 2020 : https://balkaninsight.com/2020/03/31/romanias-state-of-emergency-raises-media-freedom-concerns/
See also, OSCE, Coronavirus response bill should not curb freedom of information in Romania, stresses OSCE Media Freedom Representative, 30th March 2020: https://www.osce.org/representative-on-freedom-of-media/449380

[138] Act 300/2005 Coll. of 20 May 2005, Criminal Code of Slovakia, https://www.legislationline.org/download/id/3763/file/Slovakia_CC_2005_en.pdf

[139] Act 300/2005 Coll. of 20 May 2005, Criminal Code of Slovakia, https://www.legislationline.org/download/id/3763/file/Slovakia_CC_2005_en.pdf

[140] Act 300/2005 Coll. of 20 May 2005, Criminal Code of Slovakia, https://www.legislationline.org/download/id/3763/file/Slovakia_CC_2005_en.pdf

3.2.25 Slovenia

On 30 November 2021, no legislative measures were adopted in the country that would be directly relevant to counter disinformation. The country *takes a non legislative approach* by taking soft measures such as educational programs, media literacy activities, task forces, monitoring, support of research, etc.

3.2.26 Spain

The legal landscape in Spain changed before the general elections of 2019. The changes to Spanish Telecommunications Law (Law 9/2014) were introduced by the Royal Decree-law 14/2019 in response to the challenges of 'disinformation activities' and 'interference in political participation processes'[141].

Article 6 Section 1 of the Royal Decree law modified Article 4(6) of the Telecommunication Law, allowing the Ministry of Economy and Business to intervene, lock, or shut down the Internet and electronic communication networks or services without a previous hearing or prior judicial order in the case of 'compelling urgency' based *inter alia* on the assumption of 'an immediate and serious threat to public order, public security, or national security'. The Decree was criticised for disproportionate restriction of freedom of expression. The concepts of 'direct management' and 'intervention' are not defined; therefore, it is not clear what powers are granted to state authorities. The use of the terms 'public security' and 'national security' lacks clarity, and the concept of 'public order' can be very widely interpreted by authorities[142]. The law leaves enormous and unlimited discretion to the government, by a decision of the Ministry, in areas that should rather be dealt with by the judiciary or an independent authority'[143].

The Spanish government proposed and adopted a range of other measures to combat disinformation. In 2020, the Spanish Government approved the Ministerial Order PCM/1030/2020 Establishing the National Procedure Against Disinformation (the Ministerial Order)[144]. The Ministerial Order implements the 2018 EU Action Plan and imposes the actions and processes that the Spanish authorities must undertake to fight against disinformation. Actions are divided into categories and aim prevention, detection, monitoring, responding, analysing, and evaluating disinformation [145].

Spain does not have provisions in the Criminal Code specifically targeting disinformation. However, the 'infodemic' of COVID-19 provoked the discussion of the possible application of other criminal law provisions to false statements related to pandemics. Like other countries, the Spanish Criminal Code criminalises false statements that disturb public order. Article 561 of the Code prohibits false affirmations or simulations of a situation of danger to the community that leads to the provision of assistance to another and provokes the mobilisation of the police, assistance and rescue services[146]. There have been views that the provision could be applied in case of, for instance, possible collapse of health system which requires the intervention of police[147]. However, it is clear that the article is

[141] 'Spain: New law threatens internet freedoms', 18 December 2019, EDRI, https://edri.org/our-work/spain-new-law-threatens-internet-freedoms/
[142] 'Spain: The Royal Decree-Law 14/2019 threatens freedom of expression', Article 19, 11 February 2020, https://www.article19.org/resources/spain-ministerial-order-on-disinformation-should-favour-multi-stakeholder-approach/
[143] 'Spain: The Royal Decree-Law 14/2019 threatens freedom of expression', Article 19, 11 February 2020, https://www.article19.org/resources/spain-ministerial-order-on-disinformation-should-favour-multi-stakeholder-approach/
[144] Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional, https://boe.es/boe/dias/2020/11/05/pdfs/BOE-A-2020-13663.pdf
[145] 'Spain: The Royal Decree-Law 14/2019 threatens freedom of expression', Article 19, 11 February 2020, https://www.article19.org/resources/spain-ministerial-order-on-disinformation-should-favour-multi-stakeholder-approach/
[146] Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.
[147] Pérez, Enrique, 'El Gobierno plantea cambios legales para frenar los bulos en internet: qué castigos contempla ya la ley y por qué su regulación genera tantas dudas', 7 April 2020, https://www.xataka.com/legislacion-y-derechos/gobierno-plantea-cambios-legales-para-frenar-bulos-internet-que-castigos-contempla-ley-que-su-regulacion-genera-tantas-dudas

not suitable for most of the cases since not all cases of falsehood lead to the deployment of particular services.

3.2.27 Sweden

Sweden was known for its preventive approach through training, education and awareness raising. Spreading rumours endangering national security has been criminalised in Sweden since 1986; however, this prohibition is applicable only if the country is at war. Article 5 of the Swedish Criminal Code criminalizes dissemination among the public or the transmission or allowing to be transmitted 'to the enemy, false rumours, or other untrue assertions that are liable to cause danger to the security of the country' [148]. The crime is punishable by a fine or up to two years of imprisonment[149].

Section 15 of the Criminal Code also envisages the responsibility of raising a false alarm and imposing unnecessary safety measures. For the purposes of responsibility, the incorrect information is related to a danger to the life or health of one or more people, or to extensive destruction of property. The punishment for the crime is either fine or up to one year imprisonment[150]. This provision can hardly be applied to disinformation activities, except for extreme cases (as discussed in the context of Spanish regulation).

[148] The Swedish Criminal Code, https://www.government.se/49f391/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf
[149] Ibid.
[150] The Swedish Criminal Code, https://www.government.se/49f391/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf

3.3 Legislative measures against disinformation

When analysing the data of the questionnaire, three subcategories of legislation can be distinguished: media legislation, electoral law, and criminal law. In addition, we grouped the ongoing process into one separate category.

Figure 2: Sub-categories of the legislative activities

3.3.1 Media legislation

Under the media obligation, all the obligations of disseminating truthful information with the duty of veracity and accuracy are included. The main measures adopted under the media legislation are under the supervision of the state or an obligation for the media to respect. State supervision means that the State has prior control, as for licence regulation, which is control by the State of attribution of a licence to media, with specific criteria related to the absence of dissemination of disinformation. This is the case, for example, *Lithuania*. *Portugal* establishes a definition of disinformation and empowers the Media Regulatory Authority to assess complaints against entities and apply the sanctioning regime. *Germany* seeks to improve the enforcement of the law in social networks and places the burden on platform providers to remove illegal content.

3.3.2 Electoral law

The second subcategory, electoral legislation, is based on measures taken under the national electoral code. The prohibition of disseminating false information in the context of elections is common in *France, Latvia, and Poland*, but the means are different. In Latvia, it is a general obligation for public and private media to ensure neutrality, diversity, objectivity, and balance in reporting. In comparison, *France* and *Poland* go further by creating a specific judicial remedy. In

France, the remedy is open to prosecution, the candidate for the elections, a political party or group, and anyone interested in acting. The judge must decide within 48 hours and can take any action to prevent the dissemination of disinformation. In *Poland*, in the context of elections, the dissemination of false information is prohibited by article 111 of the electoral code. Complaints can be submitted to the district court for a preliminary ruling to prohibit disseminating such information, confiscate the material, order rectification, order publication of answer, order apology, and pay the fine of 100,000 zlotys to an organisation of public interest. In *France*, additionally, during election campaigns, an exceptional procedure for administrative suspension of the distribution of a licensed broadcasting service is established in the recently changed law on the freedom of communication. In *Spain*, the Ministry of Economy and Business can intervene, lock or shut down the Internet and electronic communication networks or services in the event of 'compelling urgency' based, among others, on the assumption of 'an immediate and serious threat to public order, public security or national security'.

3.3.3 Criminal law

In this category, all measures of criminal law are grouped. *France* establishes both a general prohibition of dissemination of false news and *lex specialis* in case of elections. *Denmark*, *Austria, France* criminalised the dissemination of disinformation in the context of elections. In *Austria*, it is punished up to six months of imprisonment or a fine of up to 360 days, whereas in *Greece* it is punished up to two years in prison or a fine. *Denmark* criminalises misinformation affecting stability of asset prices, as well as participation and assisting to influence operations. The other countries (*Italy, Cyprus, Malta*) prohibit disseminating disinformation based on threats to the public peace and order in general. In *Greece*, in addition to the context of elections, the spread of false news that raises public concern or fear or undermines public confidence in the national economy, the country's defence capacity, or public health is also punishable by up to five years of imprisonment or (and) a fine. In *Hungary*, in addition to the prohibition of disinformation based on threats to public peace, the same actions committed during an emergency legal regime and suitable for obstructing the successful defence against a danger attract heavier punishment.

3.3.3.1 Prohibited criminal conduct (Actus Reus)

There are 7 types of different prohibited conduct enacted in national criminal laws:

1. spread of any false news (Italy, Malta, Romania, Greece, Croatia, Denmark, Austria, France);
2. publish any false news (Cyprus);
3. create any false news (Croatia);
4. spread certain information: alarming news that is untrue (Czech Republic), false data or information or falsified documents (Romania), false alarming message or committing any other similar act (Slovakia), falsehood or any distorted fact any untrue fact or giving the impression that there is imminent danger for the occurrence of an event (Hungary);
5. report certain information to legal persons: a false alarming news or other similar act to a legal entity, the Police Force, other State authority or to the mass media (Slovakia);
6. provide information about danger: affirm or stimulate falsely the situation of danger to the community or producing damages (Spain).
7. evoke the activities of foreign intelligence services: commit something whereby foreign intelligence services are enabled or assisted to act immediately or directly within the territory of the state, including cooperation to carry out advocacy activities, commit the same act in the case of intelligence relating to military matters, or the enterprise takes place during war or occupation, and in connection with the elections and voting (Denmark).

Criminalization of the spread of false news is the broadest scope of enactment of disinformation in criminal law. Spreading means making false news known to others. The scope of the audience that was introduced with false news is not specified (except Hungary), but criminalization is often linked to dangerous consequences, which are different in most countries. However, only the one who spreads false news becomes liable, even though the original source of false news could not be the same one who spreads it. Therefore, the primary source of disinformation that is often related to foreign power[151] could potentially avoid liability. Except for Croatia, no other member state foreseen criminal liability also for the person who creates false news. Some of the member states limit the scope of false news related to elections (France, Austria, Denmark) or life, health, property (Spain, Greece). Others – limit the scope of spreading. For example, a criminal act is reporting certain information to legal persons or media (Slovakia). However, only a natural person could be charged with crimes related to disinformation in the EU. Legal persons could not be charged with crimes related to disinformation. Although in some it is possible to apply administrative charges through licence regulation (Lithuania)[152] or administrative sanctions (for example, Portugal, Denmark, Estonia, Latvia).

3.3.3.2 Dangerous consequences of a criminal act

Dangerous consequences as an element of crime are enacted in most countries. However, dangerous consequences could range from affecting elections to causing an economic impact. But even though the consequences are different, they are all likely to occur. It means that it is necessary to prove not the result, for example, that the public opinion formation was affected, but likelihood thereof, i.e., that spread of disinformation might influence public opinion formation or might have economical impact (Denmark). A person could not be found responsible for a crime if it is impossible to prove that disinformation could lead to specified dangerous consequences.

Table 1: Dangerous consequences of criminal acts

Dangerous consequences of a criminal act	AT	CY	CZ	DK	EL	ES	FR	HR	HU	IT	MT	RO
May influence decision-making or public opinion formation				✓								
May alarm public opinion											✓	
May prevent voters from voting or exercising their right to vote at that time	✓						✓					
May undermine public order		✓								✓	✓	
May disturb the peace and tranquility of citizens		✓	✓		✓		✓	✓	✓		✓	
May create a commotion among the public or among certain classes of the public.											✓	
May threaten national security					✓				✓			✓
May undermine public health					✓	✓						

[151] 'Source alerts can reduce the harms of foreign disinformation', https://misinforeview.hks.harvard.edu/article/source-alerts-can-reduce-the-harms-of-foreign-disinformation/
[152] C-622/17, Baltic Media Alliance v. Lietuvos radijo [2019] ECLI:EU:C:2019:566.

Dangerous consequences of a criminal act	AT	CY	CZ	DK	EL	ES	FR	HR	HU	IT	MT	RO
May undermine public confidence in the national economy					✓							
May undermine public trust towards the State or its authorities		✓										
May have economic impact				✓								
Not specified danger			✓									
Evacuation			✓									

3.3.3.3 Mental element (*Mens Rea*) of a criminal act

There are 2 types of mental element of crime enacted in national laws:

1. Malicious: Italy, Malta, Romania, Greece, Slovakia, Hungary, Spain, Austria, Croatia, Cyprus, Czech, Denmark, France.
2. Negligence: Greece, Denmark.

All member states enacted malicious acts as the mental element of disinformation-related crime. Only Greece and Denmark have enacted both: malicious and negligence. Malicious elements of crime could be both direct and indirect malicious elements. Regardless of direct or indirect maliciousness, it has to be proved that a person committing a crime knew that the information was false and wanted to spread it so as to create dangerous consequences (if it is an element of a crime). False news could be spread on media outlets, by individual journalists, famous public figures[153], bots on social media platforms, ordinary public, etc.[154]. Therefore, only a natural person could be charged with disinformation; this means that only individual journalists, famous public figures or members of the ordinary public could be found guilty of committing a crime, but not the media outlet, social networks, or organisation that funded the spread of disinformation. Malicious intent as an element of crime means that a natural person has to be aware that the information is false, understand that he/she spreads false information and do so willingly (direct intention) or having no intention for creating conditions of dangerous consequences to occur or dangerous consequences itself to occur but deliberately allows it to happen (indirect intention). The criminal codes of Greece and Denmark also enact negligence as an intent form. The main difference between indirect intention and criminal negligence is that a person did not foresee the dangerous consequences of his behaviour but due to personal qualities or the context of the situation, he should have foreseen it. While the intention to harm (*mens rea*) distinct disinformation from misinformation or other information disorder[155], it is difficult to prove it (in case a suspect is a journalist or a public figure) or almost impossible to prove it (in case a member of the general public).

[153] 'Measuring the reach of "fake news" and online disinformation in Europe', https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe
[154] https://www.bbc.co.uk/bitesize/articles/zcr8r2p
[155] European Parlament, The impact of disinformation on democratic processes and human rights in the world,2021 https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf. Council of Europe report, Information Disorder: Toward an interdisciplinary framework for research and policy making, 2017, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

3.3.3.4 Punishment

Some national criminal laws foresee serious criminal sanctions, including imprisonment up to 3 years (e.g. Hungary, Romania, Greece), in other member states violations will 'only' trigger administrative sanctions: arrest or fine[156]. The most severe punishment is enacted in the criminal code of Denmark: the person could be sentenced to up to 12 years imprisonment. National approaches also differ in what exactly is subject to regulatory intervention.

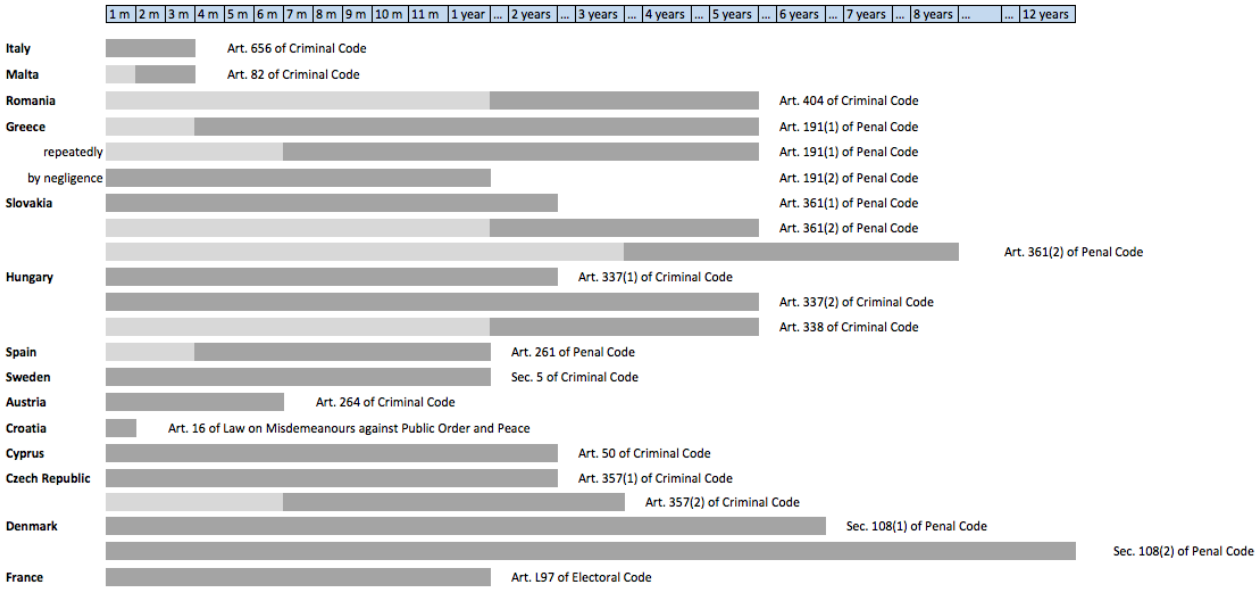


Figure 3: Punishment for prohibited conduct

[156] The perils of legally defining disinformation, https://www.econstor.eu/handle/10419/247655

Chapter 4 Cybersecurity & Information Systems Security Regulation Related to the Analyses of T-SHARK Subcases

The relevant regulatory framework to the field of cybersecurity and in terms of the Sparta project and especially T- Shark, includes the Council of Europe **Convention on Cybercrime** as well as the **EU Directives 2013/40 on attacks against information systems and 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)** in conjunction with the relevant implementing Regulation 2018/151. Since all these legislative documents are set in force in terms of European level, each member state has to adopt the introduced obligations at the national level, following its obligation to transpose the obligations and rights in terms of harmonisation.

As in terms of the operation of the subcases, information will be collected by various types of information, each of the involved member states takes the responsibility that the collected personal data will be obtained by lawful and proportionate means, also ensuring that an adequate legal ground (e.g. consent, legal obligation, etc), as required by the GDPR is in force.

4.1 The Convention on Cybercrime of the Council of Europe (the Budapest Convention)

The **Convention on Cybercrime** of the Council of Europe, known as the Budapest Convention, is to date the only internationally binding document in the field of cyber security. The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed by means of computer systems. Under these terms, the Cybercrime Convention Committee (T-CY), the monitoring body of the Convention in 2012, decided to issue Guidance Notes aimed at facilitating the use and implementation of the Budapest Convention on Cybercrime[157]. These notes will line up the basis for the analysis under legislative analysis of subcases (Chapter 6), as they specify attacks undertaken in the field of cybersecurity[158].

In general terms, the Convention on Cybercrime serves as a guideline for any country developing comprehensive national legislation against Cybercrime, as well as a framework for international cooperation between State Parties to this treaty. Following the structure of the Convention, offences in this field can be grouped into: 'a. offences against the confidentiality, integrity and availability of computer data and systems, b. computer-related offences, c. content-related offences, and d. criminal copyright infringement'. Under the Additional Protocol, the act of using computer networks to publish xenophobic and racist propaganda constitutes a criminal offence[159].

Furthermore, the treaty provides a model for mutual information exchange and formal assistance among law enforcement agencies. Article 23 of the Convention outlines the general principles for international cooperation in criminal matters related to computer systems and the collection of electronic evidence, while Article 39 of the Convention states that the provisions only supplement multilateral and bilateral treaties already effective between parties. The adoption of the Convention

[157] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[158] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[159]https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

aims to enhance harmonisation of the different national legislations and leads to reciprocal criminalization[160].

However, The Convention has come under severe criticism mainly for two reasons. First, some of its provisions fail to protect the rights of individuals effectively and secondly, it is considered in general inadequate to ensure a cyberspace free of criminal activity, by failing to address the needs of modern investigation or even supposedly infringing on state sovereignty, as some countries are non - signatory parties of the Convention[161].

4.2 The Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems

Following the aim as introduced in terms of the Budapest Convention, the Parliament and the Council of European Union, adopted **the Directive 2013/40/EU** of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (Article 15 – Replacement of Framework Decision 2005/222/JHA)[162].

In Article 3 it is mentioned that Member States shall take the necessary measures to ensure that intentional and unauthorised access to all or part of the information system is punishable as a criminal offence where it is committed in breach of a security measure, at least as of minor cases. Under these terms, **‘Attacks on information systems’** and in particular organized crime-related attacks pose an ever- increasing threat, which requires a more secure information society, as a response at the Union level, which improves cooperation of Member States at the international level, making Europe an area of freedom, security, and justice.

In Article 4 **'Illegal interference with a system',** it is mentioned that the Member States must take the necessary measures to ensure that serious interference or interruption of the operation of an information system by the introduction of electronic data, the **transmission, damage, deletion, deterioration, alteration or deletion of such data, or by denial of access to such data**, intentionally and unjustly, is punishable as a criminal offence, at least in the case of non-minor cases. Following this provision, it is possible that in case vital infrastructure is damaged or destroyed in the Union, its disruption or destruction could have a significant cross-border impact, it is necessary to strengthen the protection of vital infrastructure in the Union and as a result of national legislation from the Member States.

In Article 5 **'Illegal interference with data',** Member States shall take the necessary measures to ensure that deletion, damage, damage, alteration, or deletion of electronic data from an information system, or deliberate and unauthorised access to such data, is punishable as a criminal offence, at least in the absence of minor cases. This is a threat to achieving a more secure information society and an area of freedom, security, and justice, and therefore requires a response at Union level and improved cooperation and coordination at international level.

In Article 6 **'Illegal intercept',** Member States shall take the necessary measures to ensure that, by technical means, the non-public transmission of electronic data from, to, or into an information system, including electromagnetic emissions from an information system containing such electronic data, is intentional and unintentional. Especially, regarding large-scale cyber attacks, they can cause significant financial damage, both through the disruption of information and communication systems as well as through the loss or alteration of important commercial confidential information or other

[160] Council of Europe, Convention on Cybercrime, 23 November 2001, CETS No.185.

[161] Weber, A. M. (2003), The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425.

[162] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, OJ L 218, 14.8.2013, p. 8–14.

data, and as a result the achievement of a satisfactory level of security depends on the proper functioning and availability of information systems[163].

4.3 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

The EU Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (known as the Cybersecurity Act) is part of the European Commission's cybersecurity reform package presented in September 2017. The past three years have witnessed cybersecurity become a high priority on Brussels's agenda. The Cybersecurity Act is part of 'a set of measures across the board intended to promote more robust cybersecurity within the EU by establishing the first EU-wide cybersecurity certification framework in a broad range of products (e.g. the Internet of Things) and services[164]. On a larger scale, it falls within the development of the European Digital Single Market (DSM) strategy and improves the General Data Protection Regulation (GDPR) and the EU Network and Information Security Directive (NIS), both of which already have an important impact on cybersecurity[165].

In fact, the number of cyberattacks is still rising, and it is thus out of the question that there is a real need to strengthen cybersecurity on a pan-European level. Indeed, lack of knowledge and awareness of the end-users are factors that contribute more and more to the expansion of the target zone for the attackers and it is therefore essential to guarantee a minimum of security to protect EU citizens.[166]

It is important to mention in advance that unlike the GDPR, the CSA does not impose its certification schemes or statements of conformity. Their adoption is kept on a voluntary level, 'unless otherwise provided for in the Union law or in the law adopted by the Member States in accordance with the Union law'[167]. However, the regulation opens up to impose certification in some areas in the future and will nevertheless have an important impact on the European cybersecurity ecosystem.

The main idea behind the adoption of the Cybersecurity Act is the coordination between member states and the establishment of security certification on a European level. Article 2 of the CSA defines the European cybersecurity certification scheme as *'a* comprehensive set of rules, technical requirements, standards and procedures that are established at the Union level and that apply to the certification or conformity assessment of specific ICT products, services, or processes' [168, 169, 170].

---

[163] European Commission, Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Brussels, 13.9.2017 COM (2017) 474 final, p.4.

[164]Cynthia DONOGHUE and Howard WOMERSELEY SMITH, *Technology Law Dispatch: EU Cybersecurity Act gets the green light, June 11th 2019,* https://www.technologylawdispatch.com/2019/06/privacy-data-protection/eu-cybersecurity-act-gets-the-green-light/ .

[165] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 130.

[166] Bitkom, *Anforderungen an eine kohärente Regulierung der Cybersicherheit*, June 18th 2019, https://www.bitkom.org/sites/default/files/2019-06/20190606_anforderungen_an_eine_koharante_regulierung_der_cybersicherheit.pdf .

[167] Recital 91, Regulation 2019/881 of the European Parliament and the Council of April 17th 2019 (CSA).

[168] ICT product: "An element or a group of elements of a network or information system" (CSA Article 2)

[169] ICT service: "A service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems" (CSA Article 2).

[170] ICT process: "A set of activities performed to design, develop, deliver or maintain an ICT product or service" (CSA Article 2).

In cyberspace, cooperation, as well as strong outside-border protection, is of key importance knowing that there are no physical borders and that cyberattacks are not less harmful than physical attacks[171], thus expanding the role of the European Union Agency for Cybersecurity ('ENISA'), conferring a permanent mandate to the agency and thus strengthening its place as central interlocutor on the intra-European level regarding cybersecurity.

According to the 2016 Communication *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry*[172], *'The* cybersecurity industry in Europe has developed essentially based on national governmental demand, causing geographic fragmentation within the single digital market.' CSA shall, by pan-European certification; both 'preserve trust in the Internet' and tackle this current fragmentation[173]. For instance, in accordance with the European Commission, a person who wants to sell products in three Member States, e.g. Bulgari, Belgium and the UK, faces the necessity to be in compliance with three different certification schemes[174]. Needless to say, this leads to higher production costs for the industry.

Furthermore, the regulation aims to boost information sharing between the Member States knowing that cyber-threats are in constant mutation and evolution and that information sharing is indispensable because cybercrime does not care about borders.

According to recital 2 of the CSA 'The limited use of certification leads to individual, organisational and business users having insufficient information about the cybersecurity features of ICT products, ICT services and ICT processes, which undermines trust in digital solutions'[175].

The legal impact of the CSA and its place within the European legislative programme regarding information technology

The EU cybersecurity act is a new European regulation in the context of the development of the Digital Single Market. It entered into force for an indefinite period as of 27 June 2019 and repeals from there the regulation (EU) 526/2013 without affecting decisions taken under this regulation. However, articles 58, 60, 61, 63, 64 and 65 will only apply from 28 June 2021.

This gives, like within the framework of directives, sort of a *transposition phase* to the Member States to establish their national bodies. A clear difference between the CSA and the GDPR, whose fining system was applicable from the entry into force of the regulation, can be observed here. However, this difference finds its explanation in the fact that data protection law was already largely implemented in Member State laws before entering into force of the GDPR.

Another difference from GDPR is that the certification schemes under the CSA will **not** be mandatory. The strategy of the CSA is to establish first a voluntary system that later, due to its expected effectiveness and economic benefits, will evolve to a largely applied system by the industry. In that way, even if the ECCS is not mandatory in the beginning, the regulation sets up a gradual process towards an obligatory European certification mechanism. In fact, some industries, as explained in recital 67 of the regulation, have to have different certificates in several countries. A pan-European unified system will doubtlessly reduce their cost and, moreover, strengthen the trust of the end-users in the products, services, or processes.

[171]More on that subject: https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europet .
[172]European Commission, *Strengthening Europe's Cyber resilience system and fostering a competitive and innovative cybersecurity industry*, July 5th 2019, https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-andt .
[173] Recital 66, regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[174] European Parliament Briefing, *ENISA and a new cybersecurity act*, July 5th 2019, https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf .
[175] Recital definition: Recitals set out the reasons for the contents of the enacting terms (i.e. the articles) of an act in European legislation, EU Interinstitutional style guide, http://publications.europa.eu/code/en/en-120200.htm .

Concerning the legislative procedure, ENISA will, with the help of national experts, prepare the technical ground for the certification schemes that will then be adopted by the European Commission through implementing acts[176], and the resulting acts will be recognised in all EU Member States and 'the use of certification schemes will be voluntary unless future EU legislation prescribes an EU certificate as a mandatory requirement to satisfy a specific cybersecurity need'[177].

According to recital 94, the Member States 'should, furthermore, not introduce new national cybersecurity certification schemes for ICT products, services, or processes already covered by an existing ECCS'. Furthermore, they will have to inform the ECCG and the Commission of any new national cybersecurity laws. The impact of these changes on the CSA and the internal market will be verified by them.

The penalties within the CSA are, unlike the GDPR not capped. Article 65 only requires that they be effective, proportionate, and discouraging and that Member States, by laying down the rules on the penalties, shall, without delay notify the Commission of those rules and measures, as well as of any subsequent amendment affecting them.

The competent authority for complaints lodged by a natural or legal person will be the national cybersecurity certification authorities. The national cybersecurity certification authorities ("NCCA") have to be created by every member state and, in the field of cybersecurity, will play a similar role as the data protection authorities within the GDPR framework.

Article 64 § 2 designates the courts of the Member State in which the authority or body against which the judicial remedy is sought is located, as competent territorial jurisdiction. Natural and legal persons will as well have the right, notwithstanding any administrative or other non-judicial remedies, to an effective judicial remedy regarding decisions taken by an NCCA or a conformity assessment body concerning the improper issuing, failure to issue or recognition of an ECC held by the natural or legal person itself. Furthermore, they have the right to a judicial remedy concerning a failure to act on a complaint lodged with the NCCA or CAB[178]. Anyway, as stated before, article 65 about the penalties will only take effect from 28 June 2021.

Additionally, this document repeatedly recites some of the 110 recitals of the CSA. Recitals, unlike articles, are not per se binding rules but are, however, indispensable for the European Court of Justice ("ECJ") to interpret European legislation. Therefore, without recitals, the Court will consider the legislation as void. They are consequently of importance for the interpretation of a directive or a regulation[179].

With that in mind, recital 27 proposes "the development of a network of national education points of contact and the development of a cybersecurity training platform. The network of national education points of contact could operate within the National Liaison Officers Network and be a starting point for future coordination within the Member States"[180]. The goal of the CSA is to first increase trust in ICT products, services, and processes, and secondly 'to help prevent the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduce costs for companies operating in the digital single market'[181] Another important objective of the CSA is the stimulation of the European cybersecurity ecosystem.

As it is impossible to establish a general certificate for the entire ICT sector, the CSA lays down 'a broad and general notion of cybersecurity for the purpose of certification, which will be completed at the level of individual certification adopted by the Commission, for example, by reference to

[176] Article 49 § 7, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[177] European Commission, *DSM Fact Sheet: EU Cybersecurity Act*.
[178] Article 64, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[179] T. Klimas, J. Vaiciukaite, *The Law of Recitals in European Community Legislation*, July 2008, https://nsuworks.nova.edu/ilsajournal/vol15/iss1/6/ .
[180] Recital 27, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[181] Recital 69, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).

standards or technical specifications if no appropriate standards are available'[182]. Another purpose of the regulation is to enforce common practice regarding risk management[183].

To summarise, the CSA aims to strengthen the European cybersecurity environment by mainly establishing a European certification scheme. Therefore, it extends ENISA and advances the development of cooperation between Member States, especially with regard to the CSIRTs. Additionally, it promotes the increase in cyber awareness of EU citizens. In addition, it helps avoid the multiplication of conflicting or overlapping national cybersecurity certification schemes and thus reduces costs for companies operating in the DSM.

The impact of the CSA on the Computer Security Incident Response Teams

CSA, by strengthening ENISA, will in terms of capacity building reinforce the support to the Member States of the European Union aiming to the improvement of capabilities able to respond or even prevent cyber security infringements. It will also improve the preparedness and resilience of the EU to cybersecurity, contributing to better information sharing between EU member states through the network of CSIRTs and by organising pan-European cybersecurity exercises and training.

Article 6 (d) of the CSA reminds, as already defined by the NIS directive, that ENISA has a central role in assisting the development of national CSIRTs and that the Member States have the right to ask for assistance anytime. Furthermore, point (g) of the same article states that each CSIRT 'shall possess a common set of minimum capabilities and operate according to best practices'.

CSIRTs will also be assisted by ENISA on 'technical handling of incidents that have a significant or substantial impact through the provision of expertise, in particular, by supporting the voluntary sharing of relevant information and technical solutions between Member States'[184]. The major progress under the CSA will be the improvement of cooperation between the different national CSIRTs.

Recital 31 of the CSA shows the intention to further improve the voluntary exchange of technical information between national CSIRTs, CERT-EUs (Computer Emergency Response Team for the Institutions, Organs, and agencies) but also the private sector. The ground of this process was laid down by the NIS Directive. ENISA will also gather relevant information and act as a facilitator between the CSIRTs network and the technical community, as well as between decision makers responsible for crisis management.[185]

ENISA will prepare a regular in-depth EU Cyber Security Technical Situation Report on incidents and cyber threats for which the CSIRTs can share their own reports. In order to properly improve the cooperation between the CSIRTs and ENISA, large international cyber-exercises will be organised by ENISA.

4.4 The NIS Directive (EU) 2016/1148

As part of the security strategy, the European Commission proposed the EU Network and Information Security Directive. The NIS Directive (see EU 2016/1148) is the first piece of EU-wide cyber security legislation. The goal is to improve cyber security throughout the EU. The NIS directive was adopted in 2016 and, subsequently, because it is an EU directive, every EU member state has started to adopt national legislation that follows or ‘transposes’ the directive. EU directives give EU countries some level of flexibility to take into account national circumstances, for example, to reuse

[182] Recital 75, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[183] Recital 49, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[184] Article 7.4 (b), Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[185] Recital 32, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).

existing organisational structures or to align with existing national legislation. The national transposition by the EU member states happened on 9 May 2018[186].

The NIS Directive has three parts:

1. National capabilities: EU member states must have certain national cyber-security capabilities of the individual EU countries, e.g. they must have a national CSIRT, perform cyber exercises, etc.[187];
2. Cross-border collaboration: cross-border collaboration between EU countries, e.g., the operational EU CSIRT network, the strategic NIS cooperation group, etc.[188];
3. National supervision of critical sectors: EU Member states have to supervise the cyber security of critical market operators in their country: Ex-ante supervision in critical sectors (energy, transport, water, health, digital infrastructure, and finance sector), ex-post supervision for critical digital service providers (online marketplaces, cloud and online search engines)[189].

4.5 The NIS 2 Directive (EU)

To respond to the growing threats posed by digitalisation and the surge in cyberattacks, the Commission has submitted a proposal to replace the NIS Directive and thus strengthen security requirements, address supply chain security, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions throughout the EU. The proposed expansion of the scope covered by the NIS2, effectively obliging more entities and sectors to take measures, would assist in increasing the level of cyber security in Europe in the longer term[190]. In December 2020, the ENISA NIS investments report presented the findings of a survey of 251 OESs and DSP organizations from France, Germany, Italy, Spain, and Poland, examining their approaches to cyber security spending. The survey showed that 82 % of OESs and DSPs find that the NIS Directive has had a positive effect. However, gaps in investment still existed[191].

Subsequently, the Commission performed an impact assessment (IA) for the current proposal, which consisted of three different documents. The IA explored four different policy options for the NIS review, including the baseline option: 0) maintaining the status quo; 1) non legislative measures to align the transposition; 2) limited changes to the NIS Directive for further harmonization; and 3) systemic and structural changes to the NIS Directive. According to Article 23 of the NIS Directive, the Commission must be able to review the functioning of the NIS Directive periodically[192]. The main part of its objectives was to ensure the compliance of 'Europe fit with the digital age' by achieving that its actions will be in line with the objectives of the security union. In this framework, the Commission announced in its 2020 work program that a review would be conducted by the end of 2020. The Commission stated that 'depending on the results from the evaluation of the functioning of the NIS Directive, an open public consultation and an impact assessment will be proposed regarding measures aimed at enhancing the level of cyber security within the Union'[193].

[186] ENISA https://www.enisa.europa.eu/topics/nis-directive
[187] Maksim Iavich, Sergiy Gnatyuk, Giorgi Iashvili, Andriy Fesenko, Cyber security European standards in business, Scientific and Practical Cyber Security Journal (SPCSJ) 3(2): 36- 39 ISSN 2587-4667 Scientific Cyber Security Association (SCSA), https://journal.scsa.ge/wp-content/uploads/2019/07/03_32.pdf
[188] Ibid.
[189] Input to the Horizon Europe Programme 2021-2027 https://ecs-org.eu/documents/publications/5fdc4c5deb6f9.pdf
[190] The NIS2 Directive: A high common level of cybersecurity in the EU, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333.
[191] NIS2, https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf
[192] Ibid.
[193] Ibid.

Starting from the legal root, the legal basis for both the NIS1 and the proposed NIS2 is Article 114 of the Treaty on the Functioning of the European Union, whose objective is the establishment and functioning of the internal market by enhancing measures for the approximation of national rules. Under these circumstances, NIS2 would effectively oblige more entities and sectors to take measures, which would help to increase the level of cyber security in Europe in the long term. Taking as a basis the previously mentioned assessment and the relevant proposal for a directive on measures for a high common level of cyber security across the Union (NIS 2), which would repeal and replace the existing NIS Directive (NIS1), the proposed directive aims to tackle the limitations of the current NIS1 regime.

The proposed initiatives are summarized into three objectives: a) the incensement of the levels of cyber-resilience regarding a comprehensive set of businesses operating in the European Union across all relevant sectors, b) the reduction of inconsistencies in resilience across the internal market concerning the sectors already covered by the directive, c) the improvement of the level of situational awareness and collective capability in order to prepare and respond to the challenges arising, by also taking measures aiming at the increase of the level of trust between competent authorities in terms of sharing more information and setting of rules and procedures in the event of a large-scale incident or crisis[194].

4.6 The European Cybersecurity Certification Procedure within the CSA Framework

General information about the European certification

The technical rules on the new certification are compiled in Title III of the CSA. Article 46 states that 'the European cybersecurity certification framework shall provide a mechanism to establish European cybersecurity certification schemes and to attest that ICT products, services and processes that have been evaluated in accordance with such schemes comply with specified security requirements for the purpose of protecting the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, services, and processes throughout their life cycle'[195].

The European Commission will publish together with the European Cyber Security Certification Group ("ECCG") a 'Union rolling work programme' for certification. This programme will be a strategic document that allows industry, national authorities, and standardisation bodies, in particular, to prepare in advance for future European cyber security certification schemes. It will include a list of products, services, or processes for that certification schemes should be created or existing ones reviewed[196]. The next step for the Commission was to prepare a proposed scheme or perform a review regarding an existing one. ENISA will publish a website that provides information on and publicising European cyber security schemes[197].

Concerning the included elements of the certification, Article 54 of the CSA states that first, the certificate has to mention the subject matter and its scope as well as a demonstration about how the selected standards, evaluation methods and assurance levels correspond to the needs of the intended users of the scheme. It has also demonstrated the fulfilment of the objectives retained by article 51. The certificate must include mechanisms to demonstrate continuous and uninterrupted compliance with specified cyber security requirements and rules regarding how previously undetected cyber security vulnerabilities in ICT products, services, and processes should be

[194] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020PC0823&rid=7
[195] Radoniewicz F. (2022) Cybersecurity in the European Union Law. In: Chałubińska-Jentkiewicz K., Radoniewicz F., Zieliński T. (eds) Cybersecurity in Poland. Springer, Cham. https://doi.org/10.1007/978-3-030-78551-2_6
[196] Amendments by the European Parliament, https://www.europarl.europa.eu/doceo/document/A-8-2018-0264-AM-258-258_EN.pdf
[197] Article 50, Regulation 2019/881 of the European Parliament, and the Council of 17 April 2019 (CSA).

reported and dealt with. It shall also indicate whether conformity self-assessment is permitted under the scheme.

Regarding the issuing of the certificates, ENISA will be tasked to prepare candidate schemes (for specific groups of ICT products, processes, and services) for later adoption by the European Commission[198].

Once a European cybersecurity scheme is adopted, manufacturers or providers of ICT products, services or processes should be able to submit applications for certification of their products, services or processes to the conformity assessment body of their choice anywhere in the Union. The assessment bodies will be accredited by national accreditation bodies that control the respect of the requirements laid down in the CSA[199].

After being certified or having obtained an EU statement of conformity[200] ('ESC'), both must be accompanied by structured information that is adapted to the expected technical level of the intended end user. All such information will be available online and, where appropriate, in physical form.

Practically, the regulation proposes a traffic light system with its three levels of guaranteed certification with the provided levels basic, substantial, or high.

The CSA certified traffic light system

Article 52 of the CSA defines the three different security levels that can be ensured by certification. In that way, it established a sort of traffic light system with three levels; basic, substantial, and high. According to Article 52, the level of assurance shall be proportionate to the level of risk associated with the intended use of the ICT product, service or process, in terms of the probability and impact of an incident.

Basic level: The evaluation should at least include a review of the technical documentation of the ICT product, service, or process by the conformity assessment body[201].

The conformity self-assessment is ruled by article 53 of the CSA and the manufacturer or provider of the ICT product, service, or process has to assume responsibility for the compliance and, therefore, cooperate with the national cybersecurity certification authority referred to in article 58.

Substantial level: In addition to the requirements of the *basic level,* a verification of the compliance of the security functionalities with the technical documentation of the product, service or process is required[202]. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the products, services, or processes correctly implement the necessary functionalities[203].

High level: Adds to the requirements of the substantial level an efficiency test that assesses the resistance of security functionalities to elaborate cyberattacks carried out by people with significant skills and resources [204].

[198] MARK Young, *European Parliament approves EU Cybersecurity Act*, March 14th 2019, https://www.insideprivacy.com/international/european-union/european-parliament-approves-eu-cybersecurity-act/t .
[199] Recital 97, Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA).
[200] "An EU statement of conformity is a document that states that a specific ICT product, service or process complies with the requirements of the European cyber security certification scheme. By issuing and signing the ESC, the manufacturer or provider assumes responsibility for the compliance of the product, service or process with the legal requirements of the European cyber security scheme" (recital 97 of the CSA).
[201] Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA): Recital 88.
[202] Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA): Recital 89.
[203] Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA): Article 52.6.
[204] Regulation 2019/881 of the European Parliament and the Council of 17 April 2019 (CSA): Recital 89.

Guarantees provided by the European certification

One of the most relevant articles of the CSA regulation is, undoubtedly, article 51, which determines the security goals concerning the European cybersecurity certification schemes. According to this article, a certification will guarantee the following guarantees.

First of all, it will guarantee stronger data protection. The certificate guarantees the protection of stored, transmitted, or otherwise processed data against accidental or unauthorised storage, processing, access, disclosure, destruction, alteration, or lack of availability throughout the life cycle of the ICT product, service, or process. Second, it will ensure stronger protection regarding access rights related to the data by imposing a record of all accesses.

The certification aims as well to ensure security by default and by design, to promote update functions by default, and to make sure that security updates will be provided, every time they are needed or new vulnerabilities are known.

The benefits of the CSA for EU citizens

'Taking the example of a citizen who is considering purchasing a Smart TV and is aware of the cybersecurity risks involved when connecting similar smart objects to the Internet. In that case, EU citizens can consult the ENISA website dedicated to cybersecurity certificates. They will be able to find a model that has been certified with the appropriate cybersecurity requirements but will also find more detailed information including vendor guidance on how to set up, configure and operate the TV in a secure way and for how long the vendor commits to provide cybersecurity patches if new vulnerabilities are found'.[205]

Furthermore, ICT vendors will have the ability to better inform their clients on their security standards by using specific labels related to the certificate.

The CSA also ensures strengthened guidance for the user, as stated in Article 55. 'Manufacturer or providers of certified ICT products, services or processes shall in that way make publicly available information such as guidance and recommendations to assist end users with the secure configuration, installation, operation and maintenance of the ICT products or services, security support in a defined period, the possibility of contacting the manufacturer or provider about receiving vulnerability and a reference to online repositories listing publicly disclosed vulnerabilities'[206].

Complexity of the environment

Today, our world could be characterised as a fully electronic one, by including interconnected networks together with an enormous amount of data. Cyberspace is constantly under attack. Cyberattacks occur every second, hampering the security of a network or a device and may also vary in type and size. A cyberattack, in simple words, can qualify an attack launched from one device or more devices against another device, multiple devices, or networks[207]. Under these terms, as the majority of the organizations tries to improve their services and offer more and better services to their users, the data elements are continuously under process, connection, and comparison towards a willing result.

'Electronic systems as well as digital networks are capable of facilitating transactions, building communications, and storing personal data with reference, among others, to location, status and environment'. The goal of those launching the attack, in most cases, is to disable the targeted device, phishing emails trying to reveal the victims' passwords, as well as overwhelm a web server with traffic(DDoS) or shut it down. Sometimes, the primary goal is to get access to data stored in the

[205] European Commission, *Questions and answers – EU Cybersecurity,* June 26th 2019, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369 .
[206] https://lexparency.org/eu/32019R0881/ART_55/
[207] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf

specific device or perhaps gain administration advantages[208]. This has as a result that the noted threats in cybersecurity domain show the complexity of web business complexity, by also asking from stakeholders in cyber security domain to provide efforts concerning the flow of data in cyber security environment. Taking the above-mentioned information into account, as information systems are vulnerable to attacks and legal violations it is a necessity for them to adopt both a specified security and a privacy one.

[208] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf

Chapter 5 Data Protection and Privacy Regulation Related to the Analyses of T-SHARK Subcases

In terms of a united Europe, it is ensured that the rights of individuals as well as obligations are held by each member state, by achieving both the maximum level of harmonisation in terms of legislative procedures and relevant actions. Following this, the primary law created in terms of the EU's data protection approach is binding in all member states of the EU (controllers, processors, and data subject rights), in the form of regulation. Apart from that, there are also rules concerning data protection, which comprise on the basis of legislative and judicial initiatives, they form the secondary law and require actions as well as initiatives from each member state, providing in that way binding rules applicable in a wide range of situations.

5.1 Privacy values into cyber security policy directions

For most organisations, companies on a national level, but also in a European and international one, the affirmation that security measures will be held through their operations and activities have to be a necessity. This gap of adequate security measures finds itself confronted with the need to balance security on one hand and privacy on the other. This equation should be resolved by using the principle of proportionality.

As stated in *Protocol No 2 on the 'Application of the Principles of Subsidiarity and Proportionality' of the Treaty on the Functioning of the European Union' and in Articles 49 and 50 of the Fundamental Rights Chapter of the European Union, proportionality is a general principle of law, which is used as a criterion of fairness and justice with respect to the procedure or actions followed*. In European Union law, there are four generally acknowledged stages to proportionality which are namely: **a) legitimate aim for a measure**, **b) the measure should be suitable to achieve the aim**, **c) the measure must be necessary to achieve the aim, and d) the measure must be reasonable**.

Following this definition, it is understood that security measures that interfere with individual privacy are not acceptable, unless they are intended to meet a need related to the protection of the rights and interests of others[209]. The principle of proportionality consists in the basis for the assessment held in each particular situation, in order to figure out whether the conditions of appropriateness and necessity are met and whether the usage of the tool is compliant with the specific national and European provisions.

It can often be applied to security measures that may interfere with personal privacy, since it has to be examined in each specific case whether the measures applied are proportional and privacy friendly or not[210]. Necessity, on the other hand, implies an assessment based on the selective measure regarding its effectiveness for the objective pursued and of its intrusiveness compared to other available options for achieving the same goal[211]. Taking all these competing values into account, it is necessary to balance the competing values of privacy and security in society, which means that security measures interfering with individual privacy are not acceptable unless they are intended to meet a need that is related to protection of the rights and interests of others[212]. Where such operations have been used, the use of security systems is more likely to be considered 'proportional' in a broader range of contexts.

[209] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[210] ALADIN D3.1 Data protection, Social, Ethical and Legal Frameworks http://aladdin2020.eu/wp-content/uploads/2018/04/ALADDIN_D3.1_DataProtectionSoEL_Framework_V1_0_PU.pdf
[211] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[212] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf

Such techniques could, *inter alia*, ensure that intrusion into someone's privacy would occur only where it would be absolutely necessary or that cyberthreat intelligence mechanisms would only be activated in the presence of high-importance security reasons.

Privacy and Design

Under these circumstances, the principles of Data Protection by Design and by default are particularly important in the design and development phases of every technological project related to the gathering of large amounts of information, which might contain personal data or might interfere in one way or another with individuals private sphere. Data protection by design and by default are described in Article 25 of Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). As stated in the second paragraph of the above-mentioned article, *'The controller shall implement appropriate technical and organizational measures to ensure that, by default, only personal data that are necessary for each specific purpose of processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.'*

In the data protection context, the General Data Protection Regulation (GDPR) addressed Data Protection by Design as a legal obligation for data controllers and processors, referring also to data minimization and the possible use of pseudonymization, as mentioned in Articles 6 (d), 32 (a), and 40 of the present Regulation, as analysed below[213].

The principles of Data Protection by Design and by Default are particularly important in the development phases of every technological project related to the gathering of large amounts of information as well as for security systems, which could contain personal data or could interfere one way or another with individuals private sphere. Following this, it is necessary to affirm that the balance between privacy and security is already ensured from the early stages of the operation of the security systems and that obstacles in engaging privacy enhancement tools are eliminated. The field of application of these measures is more often observed with regard to surveillance systems that have been employed in a wider range of contents.

The notion of proportionality and the respective proportionality test, as suggested in the case law of the European Court of Human Rights (ECtHR) as provided in articles 49 and 52, with the following content: *'Any limitation on the exercise of the rights and freedoms recognized must be provided by law and respect the essence of the rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others'*[214]. Under this provision, it is understood that intrusion into someone's privacy can occur only where absolutely necessary and cyberthreat intelligence mechanisms are activated only in case an activity likely to be criminal takes place.

5.2 Data protection in European law

In terms of European legislation, legislative acts can take place both in primary and in secondary law. Regarding primary law, decisions as well as relationships between EU and its members are found in EU Treaties. Treaties are the cornerstone of EU law and are known in the EU as primary law. However, apart from the primary law, there is also the body of law that comes from the principles

[213] Ibid.
[214] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf

and objectives of the treaties and includes regulations, directives, decisions, recommendations, and opinions. Following this distinction, regulations are legal acts that apply automatically and uniformly to all EU countries as soon as they enter into force. They do not have to be transposed into national law. On the other hand, directives leave space for each member state to transpose their provisions into national law, giving space for some variation along national lines. In other words, directives have to be transposed into national legislation in terms of harmonisation and achievement of European integration. Of more practical importance are the specific legislative initiatives that the EU has taken with regard to data protection. From 1995 until May 2018, **the principal EU legal instrument was Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data (Data Protection Directive).**Until recently, these initiatives have generally taken the form of Directives that have been transposed into national law, giving space for some variation along national lines[215]. However, with the adoption of the **General Data Protection Regulation (GDPR)**, this approach is being overtaken by an effort to harmonise Member States law with the adoption of appropriate Regulations.

Legislative initiatives

5.2.1 European Convention on Human Rights - Article 8 - Right to respect for private and family life, home and correspondence

Article 8 is one of the most important articles of the European Convention on Human Rights, as it grants the right to privacy. The major impact of this article on cyberspace law is its relation to data protection. The right to privacy is protected by Article 8 of the European Convention on Human Rights which gives no explicit reference to personal data. The inclusion of this latest concept in Article 8 ECHR is the result of the jurisprudential evolution of the European Court of Human Rights on this subject, which began with the case Klass and others v. Germany.[216] With the case *S and Marper v. United Kingdom*[217] the court explicitly includes data protection in its jurisprudence related to Article 8, stating that “the protection of personal data plays a crucial role for ensuring the right to private life.”

However, the European Convention of Human Rights is not part of the EU legislation but of the Council of Europe, an international human rights organisation signed into existence by the Treaty of London in 1949. It is made up of 47 states, among which the 28 EU Member States. Even though the Convention is not part of EU law, Article 8 of the ECHR has an important impact and role in national and European jurisprudence and legislation on data protection.

5.2.2 Treaty on the Functioning of the European Union – Article 16 - Protection of personal data

The European institutions of the then *European Community* started to gain interest in data protection issues in the 1980s, when the European Commission urgently recommended the Member States to ratify Convention 108 of the Council of Europe, in order to harmonise national regulations and promote a common market in the information field.

Today, personal data are primarily protected in the Treaties of the European Union. In fact, the Treaty of Amsterdam of 1997 provided, in Article 286 TEC, paragraph 1, that 'from 1 January 1999 the

[215] Handbook on European data protection law, https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1
[216] European Court of Human Rights (Plenary), *Klass and others v. Germany*, 6th. of September 1978, application no. n. 5029/1971.
[217] European Court of Human Rights, *S and Marper v. United Kingdom,* December 4th 2008, application no. 30562/04 and 30566/04.

Community acts on the protection of natural persons with regard to the processing of personal data, and the free circulation of such data applies to the institutions and bodies established by this treaty or on the basis of the same'[218].

But it is finally with the Treaty of Lisbon that the protection of personal data has been recognised as a fundamental principle of the European Union. According to Article 16 (ex Article 286 TEC)

'Everyone has the right to the protection of their personal data. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on the European Union'. The European Union has, in fact, through Article 16 TFEU (formerly Article 286 TEC), the specific competence to protect, through ordinary legislative acts subject to the control of independent authorities, personal data of individuals. For the protection of the aforementioned rights, the European Union may also appeal, if necessary, to the Court of Justice.

5.2.3 Charter of Fundamental Rights of the European Union – Article 8

Article 8 of the Charter of Fundamental Rights now has, due to the provision contained in the new article 6, c. 1, TEU, the same legal value as the Treaties. In particular, article 8 grants everyone has the right to the protection of personal data (Article 8 (1)), establishes the core requirements for the proper exercise of the right (requirement of fairness, necessity, lawfulness, the right to access and collect the data – Article 8 (2)) and emphasizes the need for control over the restrictions of the exercise of this right Article 8 (3).

5.2.4 Regulation EU 2016/679 General Data Protection Regulation

The entry into force of Regulation 2016/679 (GDPR) has reinforced the right to privacy in all Europe. Notwithstanding that, for many companies, compliance with the GDPR is still a challenge.

The GDPR has introduced many important novelties compared to the previous directive on data protection, such as its extraterritorial application under Article 3, the concepts of privacy by design and privacy by default, or the right to data portability. Extraterritorial application means that the regulation is as well applied to data processing activities conducted by organisations that are located outside the EU. The latter have to comply with the regulation from the moment they have personal data-related activities that target the European market. Data portability however 'allows individuals to obtain and reuse their personal data for their own purposes across different services'.[219]

All these rights will, on one hand, enhance and reinforce the rights of individuals, but, on the other hand, impose new requirements for organisations when processing personal data.

As general principles, according to article 5 GDPR, every processing of personal data should comply with:

A. **lawfulness, fairness and transparency:** *'personal data shall be processed lawfully, fairly, and transparently in relation to the data subject';*

[218] SPARTA D. 10 Project results description documentation https://www.sparta.eu/assets/deliverables/SPARTA-D10.3-Project-results-description-documentation-PU-M12.pdf
[219] Information Commissioner's Office, *Right to Data Protability at a glance,* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/ .

B. **purpose limitation-** '*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, according to Article 89(1), not be considered incompatible with the initial purposes';*
C. **data minimisation-** '*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;*
D. **accuracy-** 'accurate *and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, considering the purposes for which they are processed, are erased or rectified without delay';*
E. **storage limitation -** *'kept in a form that allows identification of data subjects for no longer than is necessary for the purposes for which personal data are processed; personal data can be stored for longer periods insofar as personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation to safeguard the rights and freedoms of the data subject';*
F. **integrity and confidentiality –** *'processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures'*
G. **accountability -** *'The controller shall be responsible for and be able to demonstrate compliance with the above provisions'.*

Data processing is considered **lawful** if it takes place with respect to the following conditions (article 6 GDPR):

- the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the **performance of a contract** to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for **compliance with a legal obligation** to which the controller is subject;
- processing is necessary to **protect the vital interests of the data subject** or another natural person;
- processing is necessary for the **performance of a task carried out in the public interest** or the exercise of official authority vested in the controller;
- processing is necessary for **the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Another important principle of the GDPR is **security**. Indeed, according to article 21 of the regulation, the data controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including[220]:

a) the **pseudonymization** and **encryption** of personal data;

[220] GDPR 2021 – Compliance and Penalties; 3 Years Later, https://xypro.com/enterprise-identity-access-management/gdpr-2021-compliance-and-penalties-3-years-later/

b) the ability to ensure the ongoing **confidentiality, integrity, availability,** and **resilience** of processing systems and services;
c) the ability to **restore** the **availability** and **access** to personal data in a timely manner in the event of a physical or technical incident;
d) a process for **regularly testing**, **assessing,** and **evaluating the effectiveness of** technical and organisational **measures** for ensuring the security of the processing.

5.2.5 Directive on privacy and e-communications (e-Privacy Directive) 2002/58/EC

On 12 July 2002 The European Parliament and The European Council have adopted Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), setting as a goal the harmonisation of the required provisions of the Member States, by also ensuring an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector as well as the free movement of such data and of electronic communication equipment and services in the Community[221].

It is of high importance that the Regulatory Framework for Electronic Communications, in which the e-Privacy Directive belongs, applies to providers of electronic communications networks and services. More precisely, according to article 3, the Directive is applicable 'to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community'. Consequently, 'only services consisting wholly or mainly in the transmission of signals, as opposed to, eg, the provision of content or other value-added services' are within the scope of the Directive. The latter is not applicable to issues of law enforcement and criminal prosecution. It was adopted in 2002 and amended in 2006 and 2009[222].

However, in January 2017, the Commission adopted a new proposal for an e-Privacy Regulation, to replace the old Directive and enforce a unified approach across every Member State and type of data controller[223]. The proposed Regulation aims to address Article 7 of the CFR and would be *lex specialis* to the GDPR, tailoring data protection rules to electronic communications, including explicitly electronic communications content and metadata. ***Lex specialis,*** in legal theory and practice, is *governing a specific subject matter, 'having* as purpose to fill the gaps in general law. The scope of a special right or law is, by definition, narrower than that of a general law. The expression *lex generalis* refers literally to the 'general law'. All countries have their own definition of what is 'general law', according to the subjects studied in domestic law. It represents a general rule, a general frame, that applies in each area. In the case of two laws governing the same factual situation, the law governing a specific subject matter (*lex specialis*) overrides the law governing only general matters (*lex generalis*)[224].

A brief look at the critical aspects of the proposed Regulation is as follows: fines and sanctions would be in line with GDPR relevant provisions; also proposed to have extraterritorial effect; extends from traditional telecommunication service providers to: (i) "over the top" service providers; (ii) M2M communications (i.e. IoT technology), and (iii) probably all services with an electronic communications element; rules on direct marketing and use of cookies and other tracking technologies would apply to all marketers and websites, whereas do-not-track and anticookie wall

[221] European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2000/0189/COD.
[222] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, http://publications.europa.eu/resource/cellar/1529b684-d3d0-4445-bcdb-72f5cef237bc.0001.01/DOC_1
[223] Ibid.
[224] https://www.spacelegalissues.com/lex-generalis-and-lex-specialis/

policies would enter into force, requiring consent with few limited exceptions, for example, for security updates or audience measurement on websites[225].

5.2.6 The Directive 2013/40/EU on attacks against information systems

The Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA306 introduces rules to counterforce attacks against information systems. The objectives of this Directive are to approximate the criminal law of the Member States in the area of attacks against information systems by establishing minimum rules concerning the definition of criminal offences and the relevant sanctions and to improve cooperation between competent authorities.

Information systems are a key element of political, social, and economic interaction in the Union. Society is highly and increasingly dependent on such systems. The smooth operation and security of these systems in the Union is vital for the development of the internal market and of a competitive and innovative economy[226]. Ensuring an appropriate level of protection of information systems should form part of an effective comprehensive framework of prevention measures accompanying criminal law responses to cybercrime. The aim of these new rules is the same as the one pursued by the Cybercrime Convention: to harmonise the criminal law of the Member States in the area of attacks against information systems and to reinforce cooperation between Member States' law enforcement authorities[227].

On the definition of relevant terms, the Directive refers to:

- **'Information system'** in Article 2(a): The definition is similar to the definition of a computer system provided by Article 1(a) of the Budapest Convention, but computer data is explicitly covered by the Directive as well.
- **'Computer data'** in Article 2(b): The definition follows Article 1(b) of the Budapest Convention, which refers to an information system instead of a computer system.
- **'Legal person'** in Article 2(c): The definition covers both natural and legal persons from a liability perspective. States, public bodies, or international public organisations are excluded.
- **'Without right'** in Article 2(d): The definition addresses a general principle of criminal law and aims to avoid criminal liability for individuals acting in accordance with domestic law or with the authorization of the owner/another right holder of the information system or part of it.

New criminal offences are defined as follows:

- Illegal access to information systems in Article 3.
- Illegal System Interference in Article 4. The Directive lists eight possible acts, namely inputting computer data, transmitting, damaging, deleting, deteriorating, altering, or suppressing such data,
- rendering it inaccessible, and two possible results of the respective act, namely, severely hindering or interrupting the functioning of an information system.
- Illegal Data Interference in Article 5, which refers to any unlawful interference with computer data
- impairing its integrity or availability.

[225] ePrivacy Directive: assessment of transposition, effectiveness and compatibility with proposed Data Protection Regulation, http://publications.europa.eu/resource/cellar/1529b684-d3d0-4445-bcdb-72f5cef237bc.0001.01/DOC_1
[226] https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/2010_0273_/2010_0273_en.pdf
[227] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&rid=5

- Illegal interception of non-public transmissions of computer data and electromagnetic emissions from an information system carrying such data in Article 6.
- The illegal provision of tools used for committing the aforementioned offences is located in Article 7.

In this context, such tools could be a computer program, a computer password, or any other data allowing access to an information system[228]. The criminal liability is also extended to incitement, aiding, and abetting by natural and/or legal persons to commit as well as their attempt to commit an offence, in Article 8[229]. Incitation, aiding, and abetting cover all the offences referred to in Articles 3 – 7, whereas the attempt refers only to Articles 4 and 5. Minimum levels of penalties for offences referred to in the Directive are provided in Article 9. Taking into account that the offences mentioned above can be committed in one place while their effects might take place in another, Article 12 provides for obligations to establish jurisdiction based upon[230]:

A. the place where the offender is physically present when committing the offence;
B. the location of the targeted information system;
C. the nationality of the offender;
D. the offender´s habitual residence; and
E. the place of establishment of a legal person for whose benefit the offence is committed[231].

Concerning the exchange of information, Article 13(1) requires the Member States to establish national operational points of contact, which will be available 24 hours a day 7 days a week, and will be expected to reply to urgent requests within 8 hours after they have been addressed with a request[232].

5.2.7 Invalid Directive 2006/24/EC (Data Retention Directive)

The Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC has adopted provisions concerning the obligations of the providers of publicly available electronic communications services. In addition, public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection, and prosecution of serious crime, as defined by each Member State in its national law. However, in 2014 in the case of Digital Rights Ireland, the CJEU declared the Directive invalid *ex tunc* since it interfered with the fundamental rights to respect for private life and protection of personal data and exceeded the limits of the principle of proportionality as provided for in the Charter[233]. National legislations still need to be amended, however, only regarding aspects that became contrary to EU law after the judgement. In other words, the fact that the Directive was declared invalid does not affect the ability of the Member States under the e-Privacy Directive (2002/58/EC) to continue requesting retention of data[234].

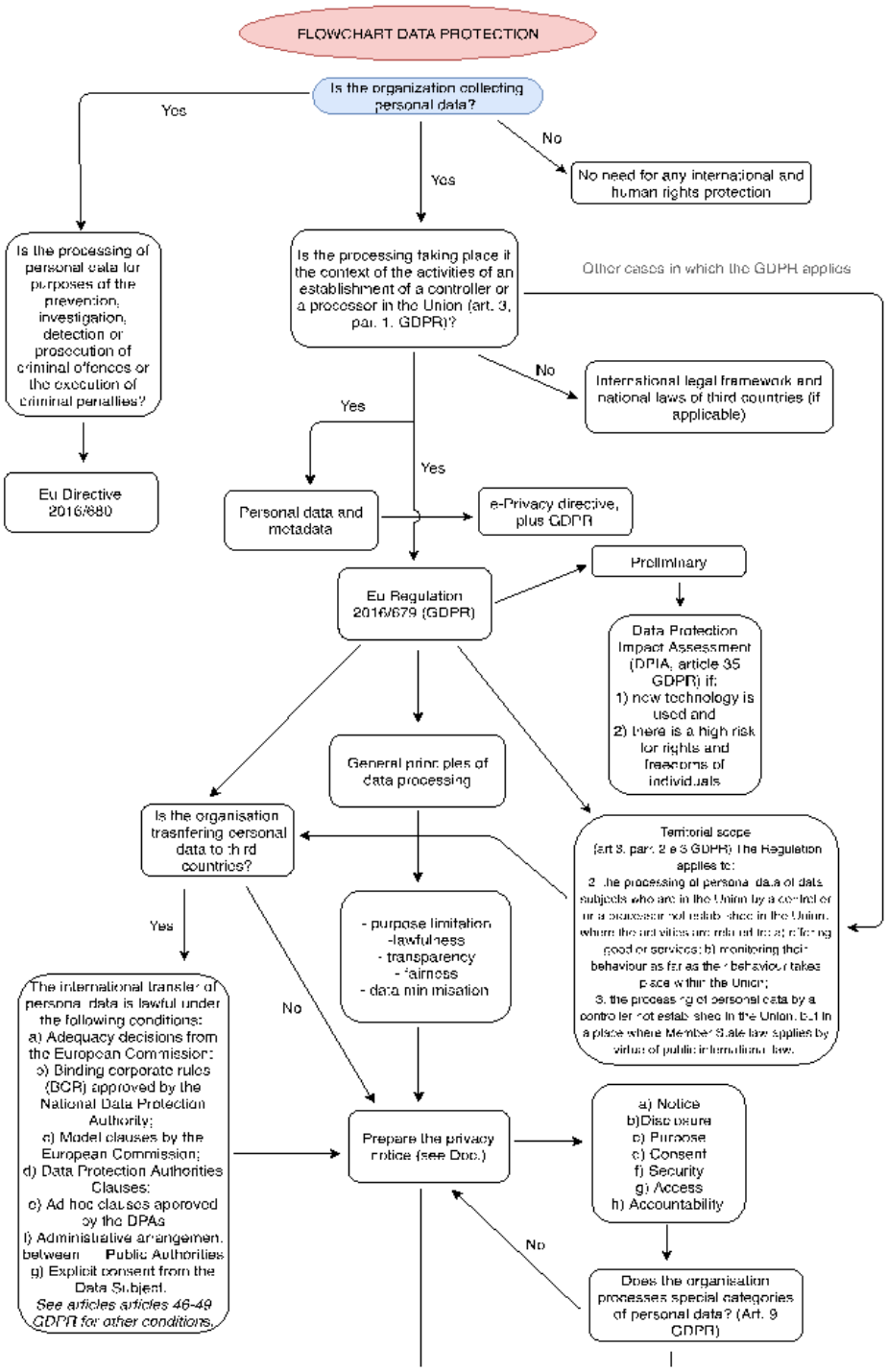
[228] Digitising Industry (Industry 4.0) and Cybersecurity, https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/607361/IPOL_BRI(2017)607361_EN.pdf
[229] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[230] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[231] Report From the Commission to the European Parliament and the Council on assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHAhttps://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0474&from=EN
[232] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf
[233] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, 13.4.2006, p. 54–63.
[234] CYBER-TRUST D3.1 Regulatory framework analysis, https://cyber-trust.eu/wp-content/uploads/2020/02/D3.1.pdf

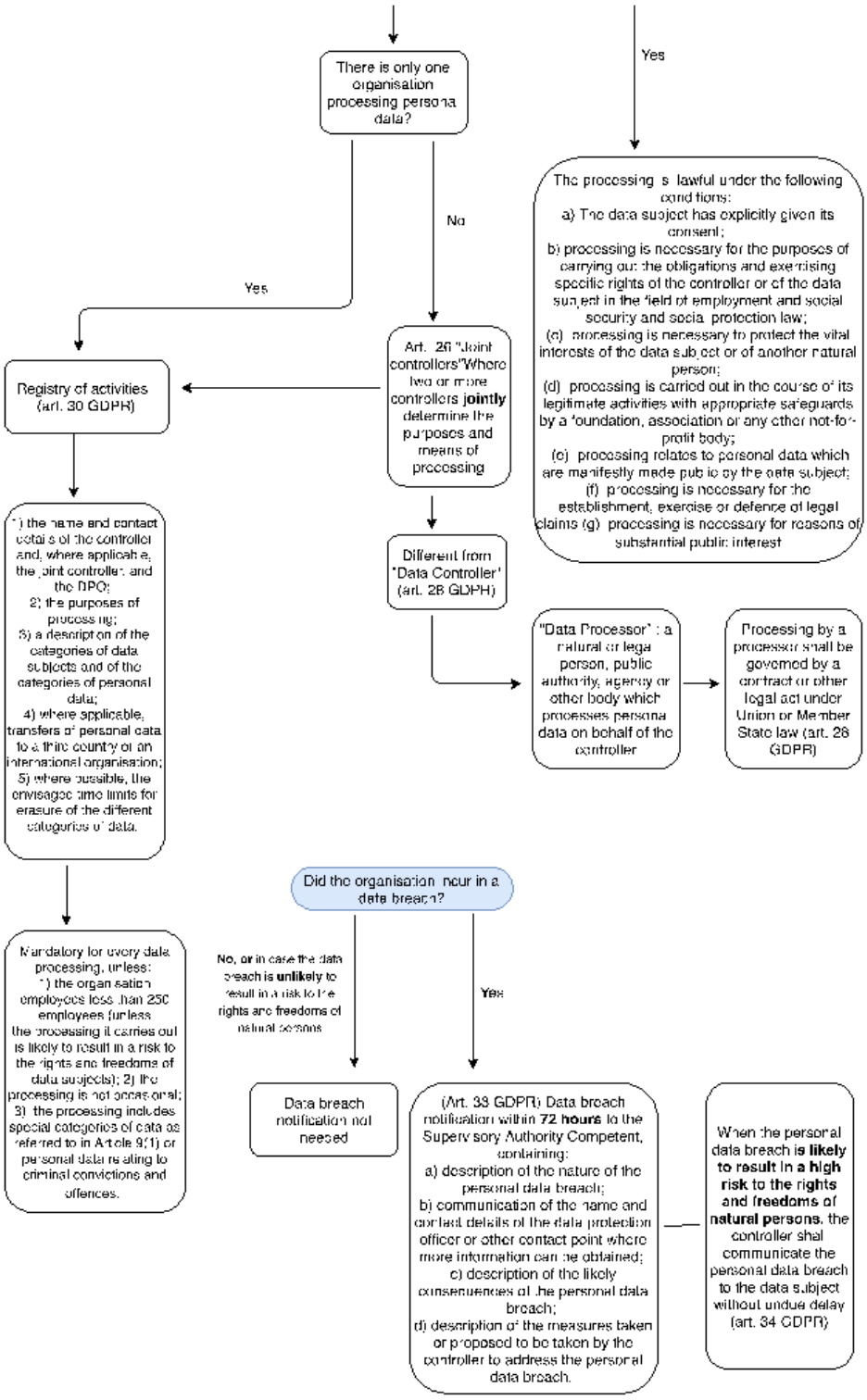
5.2.8 Directive 2009/136/EC

The Directive 2009/136/EC of The European Parliament and of The Council of 25 November 2009 amending Directive 2002/22/EC on universal service and user rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Within the framework of Directive 2002/21/EC (Framework Directive), this Directive concerns the provision of electronic communications networks and services to end users. The aim is to ensure the availability throughout the Community of good-quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market. The Directive also includes provisions concerning certain aspects of terminal equipment, including provisions intended to facilitate access for disabled end-users. This directive establishes the rights of end-users and the corresponding obligations of undertakings providing publicly available electronic communications networks and services. With regard to ensuring provision of universal service within an environment of open and competitive markets, this Directive defines the minimum set of services of specified quality to which all end-users have access, at an affordable price in the light of specific national conditions, without distorting competition. This Directive also sets out obligations with regard to the provision of certain mandatory services.

5.2.9 Data protection flow chart

The following flowchart provides an overview of the European legal framework related to the protection of personal data, in particular, the GDPR. The flowchart addresses any kind of organisation processing personal data by both identifying the main obligations under the GDPR and, identifying what to do in case of a data breach as well as potential sanctions in case of noncompliance to the GDPR.


FLOWCHART DATA PROTECTION
Is the organization collecting personal data?
Yes
No
No need for any international and human rights protection
Yes
Is the processing of personal data for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties?
Is the processing taking place it the context of the activities of an establishment of a controller or a processor in the Union (art. 3, par. 1, GDPR)?
Other cases in which the GDPR applies
No
International legal framework and national laws of third countries (if applicable)
Yes
Eu Directive 2016/680
Personal data and metadata
Yes
e-Privacy directive, plus GDPR
Eu Regulation 2016/679 (GDPR)
Preliminary
Data Protection Impact Assessment (DPIA, article 35 GDPR) if:
1) new technology is used and
2) there is a high risk for rights and freedoms of individuals
General principles of data processing
Is the organisation trasnfering personal data to third countries?
Territorial scope (art 3, par. 2 e 3 GDPR) The Regulation applies to:
2. the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union, where the activities are related to: a) offering good or services; b) monitoring their behaviour as far as the behaviour takes place within the Union;
3. the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
Yes
- purpose limitation
-lawfulness
- transparency
- fairness
- data minimisation
The international transfer of personal data is lawful under the following conditions:
a) Adequacy decisions from the European Commission;
b) Binding corporate rules (BCR) approved by the National Data Protection Authority;
c) Model clauses by the European Commission;
d) Data Protection Authorities Clauses;
e) Ad hoc clauses aproved by the DPAs
f) Administrative arrangemen. between Public Authorities
g) Explicit consent from the Data Subject.
See articles articles 46-49 GDPR for other conditions.
No
Prepare the privacy notice (see Doc.)
a) Notice
b)Disclosure
c) Purpose
c) Consent
f) Security
g) Access
h) Accountability
No
Does the organisation processes special categories of personal data? (Art. 9 GDPR)


There is only one organisation processing personal data?
Yes
No
Yes
The processing is lawful under the following conditions:
a) The data subject has explicitly given its consent;
b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
(c) processing is necessary to protect the vital interests of the data subject or of another natural person;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims (g) processing is necessary for reasons of substantial public interest
Art. 26 "Joint controllers"Where two or more controllers jointly determine the purposes and means of processing
Registry of activities (art. 30 GDPR)
Different from "Data Controller" (art. 28 GDPR)
"Data Processor" : a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller
Processing by a processor shall be governed by a contract or other legal act under Union or Member State law (art. 28 GDPR)
1) the name and contact details of the controller and, where applicable, the joint controller and the DPO;
2) the purposes of processing;
3) a description of the categories of data subjects and of the categories of personal data;
4) where applicable, transfers of personal data to a third country or an international organisation;
5) where possible, the envisaged time limits for erasure of the different categories of data.
Did the organisation incur in a data breach?
No, or in case the data breach is unlikely to result in a risk to the rights and freedoms of natural persons
Yes
Mandatory for every data processing, unless: 1) the organisation employees less than 250 employees (unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects); 2) the processing is not occasional; 3) the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences.
Data breach notification not needed
(Art. 33 GDPR) Data breach notification within 72 hours to the Supervisory Authority Competent, containing:
a) description of the nature of the personal data breach;
b) communication of the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) description of the likely consequences of the personal data breach;
d) description of the measures taken or proposed to be taken by the controller to address the personal data breach.
When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay (art. 34 GDPR)

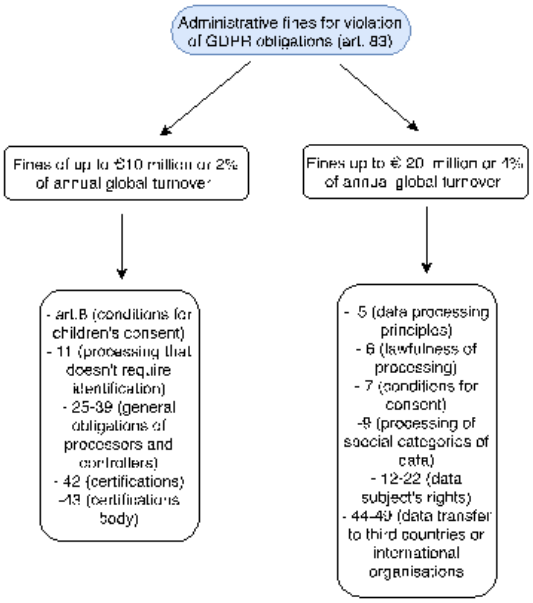


Figure 4: Data protection flow chart

Chapter 6 Analyses of T-SHARK Cybersecurity Threat Prediction Subcases

6.1 Detection of cyber and physical attacks on critical infrastructure across Europe (INOV/LIST)

General information about the subcase

The quality of life of EU citizens and their security, as well as the correct functioning of the internal market, depend on the reliable functioning of critical infrastructures in a wide range of sectors. This requires that adequate efforts are taken to protect key infrastructures from disruptions[235]. However, should this fail, critical infrastructures must be resilient, to adequate performance levels within a reasonable amount of time. Under these terms INOV with the collaboration of LIST, IST, and TCS proceeded to the creation and analysis of its subcase which operation is thoroughly described below:

In recent years, industrial control systems (ICSs), such as those involved in manufacturing, transportation, energy production, and distribution have been affected by cyber-physical attacks. On the one hand, the window of opportunity seems to be justified by the increased number of IT devices introduced in ICSs, which create an attack surface that can be used to launch these attacks. On the other hand, the effectiveness of these cyberphysical attacks can be related with the fact that conventional intrusion detection systems (IDS) fail to detect these cyber threats, missing the opportunity of triggering a prompt reaction. Failure to detect cyber-physical attacks targeting ICS devices occurs because they often abuse legitimate actions to lead the ICS into an invalid physical state. Examples include continuously turning off physical equipment to cause denial of service or altering configurations, like equipment operation speed, to compromise the ICS security and dependability. Such attacks often impact the integrity of ICS devices, which may lead to industrial process faults. The faults may raise dependability concerns related to service integrity, availability, and reliability. Given that these actions in the right context are legitimate, many intrusion detectors are unable to mention them as malicious. Signature-based IDSs are particularly inadequate to deal with these cases when legitimate and illegitimate actions are hard to differentiate, as they are based on descriptions of malicious behavior (signatures). An alternative solution to this problem is anomaly-based IDSs. These detectors model the normal behavior of the monitored infrastructure by observing its operation during a learning period, while also detecting relevant deviations from that model. These IDSs have two issues: (1) the model only reflects the operations that were seen during the learning period, making the IDS prone to false alarms; (2) the model is typically constructed using a machine learning approach, so it is hard to understand by humans, making it difficult to interpret the raised alarms. A third solution is specification-based IDSs (SBIDS). They detect deviations from a specification of the behavior of the system or protocol, so their alarms are interpretable. However, these specifications are typically created by humans, which is a deterrent to this intrusion detection approach.

With regard to the information gathered as an answer to the questions set in the Questionnaire prepared by KEMEA in collaboration with Smile in the scope of Legal Analysis of T-Shark Subcases, this use case focuses on designing novel methods that provide five classes of the threat model for addressing cyber-physical threats on ICSs:

[235] Inception impact assessment, https://pracodawcy.pl/wp-content/uploads/2020/06/Wst%C4%99pna-ocena-skutk%C3%B3w-Ares20203202859.pdf

1. Collection

An automated method is being constructed to collect specifications based on network traffic. This method, named FINGERICS, automatically generates a fingerprint model of an ICS system based on network traffic inspection, business process discovery, and physical behavior analysis. The fingerprints provided by this solution can be used to configure specification-based IDS, and in this way reduce the amount of human effort required to detect malicious activity. Furthermore, the fingerprints obtained by FingerICS serve as the rule sets for cyber-physical threat analysis.

2. Detection

A threat detection system, Business Process-Based Intrusion Detection System (BP-IDS), is being developed capable of identifying security incidents in SCADA networks based on the specification of ICS devices and industrial processes. The detection system allows experts to model industrial processes as business processes, represented as Business Process Modelling Notation (BPMN) diagrams. BP-IDS uses these diagrams as a security policy to identify exploited threats. Identifies operations in logs or network traffic based on multiple sensors scattered on the monitored ICS infrastructure. Operations indicate the execution of activities in business processes and match in real-time the operations detected in the executed business process with the specified business process and specified business rules of the specification[236]. Whenever those executed processes deviate from the specification, the activity is marked as a possible incident, and the infrastructure administrator is notified in real-time by BP-IDS with the causes of that anomaly (traces, affected processes, etc)[237]. BP-IDS also allows experts to model the physical components of the infrastructure using unified modelling language (UML) class objects. The key attributes of the UML objects are used to identify the physical systems on the collected traces, and non-key attributes maintain the state of those systems. Experts can also express as security policy the conditions for activity execution by writing logic programming rules that correlate non-key attributes with activity execution. Thus, BP-IDS can validate that the expected valid physical state of the ICS is maintained throughout the execution of the monitored industrial process. This SBIDS has been used for detecting anomalies on the public information system of a rail transportation network, false data on HMIs of gas distribution networks; GDPR compliance on Local Public Administrations; and airport systems. The tool offers a broad detection of cyber security incidents (such as intrusions or forgery of equipment behavior) and dependability faults (like, equipment and network failure, human error, or natural disasters)[238].

In the INOV subcase, an extension of mission-aware impact assessment models is proposed to incorporate information from multiple intrusion detection systems such as Snort or Ossec, as well as other security and safety alarms such as firewalls or physical sirens[239]. Starting from the augmented VTAC, two additional dependency layers will be added: a physical layer to further include cyber-physical to the organization layer that is the typical entry point for attacks occurring in SCADA networks. The physical layer will assess the state of physical components by calculating the impact of the physical assets of the organization. Furthermore, since cyber security incidents and risks can no longer be supervised at the individual critical infrastructure level, a holistic dimension of the approach will be investigated. This will also require the formal identification of interdependency links between critical infrastructure that can lead to the mechanism of propagation of an event within a critical infrastructure towards remote dependent critical infrastructures, as well as the method and associated algorithms for event propagation. The information thus exchanged will feed a local

[236] SATIE D4.1 - Specification of data exchanges, interfaces and log semantic, https://satie-h2020.eu/wp-content/uploads/2021/02/SATIE_D4.1_Specification-of-data-exchanges-interfaces-and-log-semantic_PU_v2.0.pdf

[237]

[238] SATIE D4.1 - Specification of data exchanges, interfaces and log semantic, https://satie-h2020.eu/wp-content/uploads/2021/02/SATIE_D4.1_Specification-of-data-exchanges-interfaces-and-log-semantic_PU_v2.0.pdf

[239] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

prediction engine, to allow the analysis of the current and upcoming situation based on local data and data from the critical infrastructure ecosystem. AI technologies need to be completed with privacy-preserving tools such as Holomorphic Encryption (HE) and Private Aggregation of Teacher Ensembles (PATE) approaches, in order to be able to exploit confidential data all along the lifecycle of AI methods, with a focus on the learning step[240].

Relevant legal regulation for the subcase analyses

Under this framework, there exists the observance that AI technologies need to be completed with private-preserving tools such as Holomorphic Encryption (HE), and Private Aggregation of Teacher Ensembles (PATE) approaches, in order to be able to exploit confidential data all along the lifecycle of AI methods, with a focus on the learning step. PATE provides a layer of privacy for the model, but instead there arise limitations[241]. The first one is that the trust is channelized into a third party, while this is not an acceptable option for obvious privacy reasons. Furthermore, this approach allows parties to add a confidentiality layer by using holomorphic cryptosystems, which solves the trust problem created among the involved parties from a legal point of view.

Visualization, Prediction, and Hypothesis Building - An impact assessment method, Business Impact Assessment (BIA), capable of simulating threat propagation in ICS infrastructures, and evaluating the possible impact a cyber-threat can have on the industrial processes of the organization. This is achieved by modelling threats on ICS devices using STRIDE or MITRE ATT&CK methodologies, which map the ICS specifications with the threats identified for the ICS devices.

In terms of addressing the European initiatives, which took place among the last years, the European Commission in its European Programme for Critical Infrastructure Protection (EPCIP) of 12 December 2006, set out an overall policy approach and framework for critical infrastructure protection (CIP) activities in the EU against all hazards and in all sectors. The four main focus areas of EPCIP are

- a procedure to identify and designate European critical infrastructures and assess the need to improve their protection limited to the transport and energy sector;
- measures to facilitate the implementation of the EPCIP, including expert groups at EU level, an information-sharing process, and a Critical Infrastructure Warning Information Network (CIWIN);
- research on and subsidies for CIP-related measures and projects; and
- a framework for the cooperation with third countries[242].

Following this, the Council of the European Union on 8 December 2008 adopted the Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. According to article 1 “This Directive establishes a procedure for the identification and designation of European critical infrastructures ('ECI'), and a common approach to assessing the need to improve the protection of such infrastructures in order to contribute to the protection of people”[243]. Apart from that, the proposal for additional measures on critical infrastructure protection is included in the Commission work program 2020. Regarding the answer provided in Part 4 of the questionnaire, the organization ensures that *“The tools developed in this subcase are compatible with the critical infrastructures described in the directive 2008/114/EC. In particular, BP-IDS and BIA have been field tested on transports (aviation and railways) and on the energy sector (gas pipeline distribution)”.*

[240] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf
[241] Ibid.
[242] Inception impact assessment, https://pracodawcy.pl/wp-content/uploads/2020/06/Wst%C4%99pna-ocena-skutk%C3%B3w-Ares20203202859.pdf
[243] Evaluation Study of Council Directive 2008/114 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection– Final Report

Regarding the data used, they are relevant with the file logs or network traffic. Taking this into account, the data is used to monitor the activity of the critical infrastructure and detect anomalies that compromise the physical operations of the infrastructure. It is not common for data to contain sensitive personal information. Moreover, they will be collected and based on a laboratory experiment, which simulates a critical infrastructure, and not on real data. Taking this into account, the data collected while monitoring is stored in the tool's internal storage. When an abnormality is detected, the data related to this are shared to other T-SHARK partners using the C3ISP and MISP platform. Since the data collected are based on a laboratory experiment, there will be no foreseen risk of maintaining the data after the project conclusion. This need will be further revised on the month of the project in order to erase the unnecessary data obtained throughout the project. Since the data obtained are based on laboratory experiments, there will not be any personal or sensitive data monitored by the subcase tools. Following this, the tools are crafted in order to take into account privacy by design, and do not require any personal data to be stored or processed by default. Some tools such as BP-IDS can also be used aiming to monitor personal data, but in this case they would require additional configuration from administrators. Finally, since the data obtained are based on laboratory experiments, there will not be any personal or sensitive data monitored by the subcase tools.

Problems that must be tackled

Taking into account all the above-mentioned issues and legislative initiatives, it is noted that the existing framework for protection and resilience of critical infrastructures is inadequate in the light of increasing interdependencies and evolving risks. As these infrastructures are more dependent on one another, disruptions in one sector can have immediate and, in some cases, long-lasting effects on operations in others. As a result, services that are essential for the maintenance of critical societal and/or economic activities can be significantly disrupted. Moreover, some of the disruptions can have severe and cross-border consequences for security and lead to uncertainty or undermine confidence in the responsible authorities and providers of essential services. Therefore, the proposed initiative will aim to address the following aspects that were identified in the recent evaluation of the ECI Directive and subsequent discussions with stakeholders:

1. Discrepancies in the implementation of the ECI Directive, which leaves broad space for interpretation, leading to a wide variance in national approaches and uneven designation of European critical infrastructures.
2. Insufficient focus on resilience of critical infrastructure at European level: A single focus on physical protection does not ensure reliable functioning of critical infrastructures.
3. Risk assessment methodologies appear in a variety of forms. The threat picture facing critical infrastructures comprises terrorism, hybrid actions, cyber-attacks, insider incidents; potential threats associated with new and emerging technologies (such as drones, 5G, artificial intelligence), or disruption of supply chains. There are a range of different procedures, methodologies, and coordination mechanisms in place in member states and within sectors aimed at assessing and addressing different threats/risks, which in some cases do not necessarily reflect the evolving risks[244].

[244] Inception impact assessment, https://pracodawcy.pl/wp-content/uploads/2020/06/Wst%C4%99pna-ocena-skutk%C3%B3w-Ares20203202859.pdf

6.2 Heuristics for observation of DDoS around the world / Advanced methods for DDoS profiling (CESNET)

General information about the subcase

The objective of the subcase is to utilise the backbone network hosting several / 16 prefixes as an observation point for the backscatter traffic. In such a case, it is not possible to use raw packet capture as a source of data but the subcase will use flow collected from the edges of the backbone to collect all back-scatter traffic flowing through the backbone. Machine learning methods will be employed to train heuristics which will classify back-scatter and no-back-scatter traffic.

The DDoS backscatter traffic tool allows real-time identification of a single victim of a DDoS attack by identifying their IP. It is a tool for identifying low intensity DDoS attacks in real-time with the accuracy of a single IP address.

Relevant legal regulation for the sub-case analyses

The EU Directive 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (The Police Directive). The Directive aims at establishing rules relating to the protection of natural persons with regard to the processing of criminal offences or the execution of criminal penalties, including the safeguarding against and prevention of threats to public safety. The Budapest Convention on Cybercrime establishes the criminalization requirements for computer-related offences within the EU.

The EU Directive 2016/680 stipulates the following requirements for data processing of DDoS backscatter:

1. Data processing and sharing can only be conducted between competent authorities; in the case of the subcase, the competent authority would be national CERTS.
2. The personal data should be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with these purposes, for the purposes of prevention, investigation, detection or prosecution of criminal offences.
3. The personal data collected should be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.
4. Distinction has to be made between different categories of data subjects – suspects, convicted criminals, victims, and third parties such as potential witnesses
5. Automated decision making on the processing of data that has significant implications on the data subject is prohibited without providing human intervention possibilities to safeguard the data subjects rights and freedoms.

These requirements pose specific restrictions for CERTS to follow and implement in their daily operations to be able to exploit the DDoS backscatter detection model in their activities.

The implementation of the Police Directive further dictates that the act for which the data is being processed is considered a criminal act. Within the EU cybercrimes are defined in the Budapest Convention on Cybercrime.

The Budapest Convention on Cybercrime establishes internationally recognized elements of cybercrime. In order to process personal data within the EU as per the Law Enforcement Directive, the goal of the processing of data needs to be for the prevention, investigation, detection, or prosecution of criminal offences. The Budapest Convention establishes these criminal offences for cyberspace.

1) In order to process personal data in identifying a victim of a DDoS attack, the DDoS attack needs to be recognized as a criminal offence by the state where the offence takes place, and the data needs to be processed by the same state's competent authority.
2) The Budapest Convention on Cybercrime Article 5 'System Interference' establishes the obligation for signatories of the Budapest Convention to adopt national measures that are necessary to establish a criminal offence, serious hindering without the right to the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.
3) The Budapest Convention adds the following requirements in determining the legal use of DDoS Backscatter Traffic Detection technology to identify ongoing victims of DDoS attacks:

   a) The DDoS attack is recognized as a criminal offence in a member state national law;

      and

   b) The volume of the DDoS attack currently in progress is sufficient to fall under the relevant national law.

Conclusions and recommendations

The main obstacle in universal implementation of the proposed DSos backscatter traffic detection models stems from the Member States national laws and whether or not low-intensity attack on an individual IP or computer falls under national definition of cybercrime. The law enforcement directive grants the permission to process data for the purposes of detecting ongoing crime for criminal offences. Therefore, Member State national legislation does not accept low intensity DDoS as a cybercrime, and the module could not be implemented in detecting low intensity DDoS attacks. However, this does not restrict the implementation of the module to detect significant interferences that stem from DDoS attacks. National regulations need to be observed very carefully in order to implement the technology in different Member States, or a consideration of adopting legislation that recognises DDoS attacks on an individual IP or computer should be adopted.

6.3 Threats and attacks analysis (EUT)

General information about the subcase

The present subcase is centred in supporting law enforcement institutions in their actions to investigate and prosecute criminal organisations for launching cyberattacks, focusing on the search of similar behaviours from the tactics and strategies used in the different attacks (represented by ATT&CK). The aim is to automatically (or pseudo-automatically) find relationships between threats and attacks in order to carry out the process of attributing malicious actions to an organised group (criminal, terrorist, state). This can be achieved through the detection of common origins between threats and attacks. In the subcase, the following challenges are addressed: a) The exhaustive characterisation of relevant variables and factors, both general and exclusive to each domain, that proves to maximise the collection and analysis of information in threat intelligence strategies for active defence, b) Research of habitual techniques for the construction of behaviour models of attacks that have been detected and characterised (attack model), c) Implementation of automatic learning techniques and algorithms, whether supervised or unsupervised, to group similar threats/attacks, which could be indicative of coming from the same source, and for the definition of commitment indicators that refer to the groups determined in the previous point.

The subcase ‘Analysis of threats and attacks’ focuses on supporting law enforcement institutions in their actions to investigate and prosecute criminal organisations for launching cyberattacks, while in terms of establishing the actor (or actors) responsible for a threat or attack, a thorough

characterization of relevant attributes and factors should be performed to find relationships between threats / attacks automatically (or pseudo-automatically)[245].

Afterward, a machine learning algorithm maps a group (or groups) to the tactics, techniques, and/or procedures reported involved in one threat.

Relevant legal regulation for the sub-case analyses

The subcase 'Analysis of threats and attacks' focuses on supporting law enforcement in their actions to investigate and prosecute criminal organisations that launch cyberattacks. In order to establish the actor (or actors) responsible for a threat or attack, a thorough characterization of relevant attributes and factors should be performed to find relationships between threats / attacks automatically (or pseudo-automatically). In these terms, expert analysts often analyse digital forensic evidence and also historical data, establishing intentions, reasons, or motives, and taking the overall situation into account. A TTP (Tactics, Techniques, and Procedures) describes how to analyze an advanced persistent threat (APT's operation) and can also be used to profile a certain threat actor. Following the answers provided by EUT in the questions set in the distributed questionnaire, the MITRE ATT&CK knowledge base describes an attack from an attacker's point of view, providing knowledge of the attacker and its profile. The organisation ensures that its actions are in accordance with the privacy and security legal obligations set by the law. Hence, the events are uploaded to MISP by the owners of other subcases. In these terms, the purpose of data processing is to determine behaviour patterns of the actor (or actors) responsible for a threat or attack. The MISP events are analysed but not saved in any external place, while the resulting software asset will have a licence property of Eurecat and a static security analysis of source code will be performed.

6.4 Modern Approach to Malware Analysis Automation (NASK)

General information about the subcase

The overall objectives of the subcase are the development of automated tools that support malware analysis on all stages, tracking the development of malware families, and understanding the modus operandi of actors behind them. This will be achieved through the development of solutions to support malware analysts in assessing the type and functionality of the investigated samples. Specifically, the selected approach focuses on the detection of similarities between malware codes on various levels: entire unpacked (de-obfuscated) samples, functions, and basic blocks. The subcase includes multiple methods of comparison: lexical analysis of decompiled code, comparison of normalised disassembly representation, API usage, control-flow graphs, and more. Beyond facilitating the analysis of individual samples, it enables improved situational awareness and prediction capabilities through analysis of the overall development trends in the many malware families that are monitored by CERT.PL and other researchers. The prototype will be integrated with the CERT.PL created online malware analysis and information sharing service - mwdb.cert.pl – which will make the results of the analyzes available to the research community. The second type of integration will focus on popular tools for reverse engineering, such as IDA Pro and Ghidra, to annotate individual functions with additional metadata that significantly speed up the process of manual analysis[246].

[245] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf
[246] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

Relevant legal regulation for the sub-case analyses

Regarding the specific domain, the following legislative initiatives were performed:

1. The EU Directive 2016/1148, Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 'NIS Directive'[247]: The directive aims at promoting a high level of network and information system security within the EU. The provisions are driven by a cross-sectoral approach that requires operators of essential and digital services to take appropriate security measures and to notify serious security incidents to public authorities of the Member States. It also requires member states to implement cybersecurity strategies and creates new mechanisms for cooperation among them (cooperation network, strategic cooperation, and CSIRTs network, operational cooperation)[248].
2. The Cybersecurity Strategy of the EU (CSS): one of the initiatives of the DSM strategy and the first EU-level strategic document dealing with cybersecurity. Creating cyber resilience and reducing cybercrime are some of the main goals. The document stresses the importance of cooperation between different stakeholders.
3. The European Commission Recommendation on Coordinated Response to Large-Scale Cybersecurity Incidents and Crises ("Blueprint"): The identified goals are: 1) Strengthening cooperation to improve preparedness and deal with cyber incidents 2) Addressing the challenges facing the Europe's cybersecurity single market and 3) Nurturing industrial capabilities in the field of cybersecurity. Focusing on cooperation and training within and between member states.

Regarding the data protection sector, the below-mentioned legislation is applicable:

1. The EU Regulation 2016/679, on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 'General Data Protection Regulation - GDPR'. CSIRTs must consider GDPR limitations when sharing personal data between their constituency and with other authorities;
2. The EU Directive 2002/58249 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications);
3. The EU Directive 2016/680 on the Protection of Natural Persons with respect to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection, or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data (Law Enforcement Data Protection Directive - LE DP Directive);
4. The EU Directive 2016/681 on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crimes (Directive on the Use of Passenger Name Record – PNR - Data).

Legal Problems that have to be tackled

The diversity of national legal frameworks and the complexity in the transposition, implementation, and enforcement of EU law are the main legal challenges hindering the cross-border and cross-sectoral cooperation between CSIRTs and law enforcement. For example, the substantive laws of Member States may define differently a specific incident, which in certain jurisdictions may be not

[247] https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[248] ENISA, Legal and Organisational Aspects of Cooperation Between CSIRTS and LE, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/cooperation-across-csirts-and-law-enforcement/support-the-fight-against-cybercrime-training-material-legal-org-aspects-of-csirt-le-coop-handbook.pdf
[249] https://www.legislation.gov.uk/id/eudr/2002/58

considered as a criminal offence. Furthermore, data retention periods and the scope of data retention can vary significantly in addition to the procedural powers of law enforcement in obtaining electronic evidence. During the transposition period, efforts and adjustments of the national legal frameworks are required in order to implement newly introduced EU legislation. In addition, there might be some challenges related to the implementation of specific pieces of legislation itself. Notably, examples of such implications arise from the transposition of the NIS Directive and the LE Data Protection Directive, as well as from the implementation of the GDPR[250]:

1. NIS Directive: All member states have published a national cybersecurity strategy. However, it remains to be seen whether all member states provide sufficient resources to CSIRTs and competent authorities to ensure a high level of network security.
2. The Law Enforcement (LE) Data Protection Directive includes increased cost requirements in terms of both the staffing and technical means necessary to ensure compliance with the provisions of the Directive.
3. GDPR: Proper application of Article 23 and Recital 49, which allows the collection and processing of personal data by CSIRTs without the consent of the data subject. Without due consideration of the recital, the CSIRT and law enforcement cooperation could become more difficult.

Organisational Problems that have to be tackled

The causes of organisational challenges faced in the cooperation between stakeholder entities have been identified as follows:

1. Lack of skilled personnel: Limited skilled staff is placed both on the side of LE and CSIRTs as the demand for cybersecurity professionals in the private sector is greater.
2. Insufficient training: Limited training opportunities and resources, especially for conducting common training for both communities. Training should focus on both technical, organisational, and legal aspects.
3. Lack of agreed procedures on information sharing: There are often no defined procedures to identify criminal offences or to fulfil the obligation to share information/data.
4. Lack of knowledge of international standards: Very limited knowledge of the available ETSI, ISO, and NIST standards, which could facilitate cooperation.
5. Lack of trust: This is the main reason for the lack of cooperation. Building and maintaining trust is a process that requires investment of resources and time.

Steps forward

In order to increase our chances of bringing perpetrators to justice, we need to urgently improve our capacity to identify the persons responsible for cyber attacks. Finding useful information for cybercrime investigations, mostly in the form of digital traces, constitutes a major challenge for law enforcement authorities[251]. We therefore need to increase our technological capability trying to investigate effectively with reference, among others, to the reinforcement of Europol's cybercrime unit together with cyber experts. Following this, Europol has become a key actor in supporting Member States' multijurisdictional investigations, aiming also to become the centre of expertise for Member States' law enforcement regarding both online investigations and cyber forensics.

[250] ENISA, Legal and Organisational Aspects of Cooperation Between CSIRTS and LE, https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/cooperation-across-csirts-and-law-enforcement/support-the-fight-against-cybercrime-training-material-legal-org-aspects-of-csirt-le-coop-handbook.pdf

[251] Handbook on cybersecurity, https://www.bundesheer.at/pdf_pool/publikationen/hb_on-cyber-defence-2-auflage_web.pdf

It is common knowledge that the widespread practice of placing multiple users behind one IP address makes it technically very difficult to investigate malicious online behaviour. It also makes it sometimes necessary, for instance, for serious crimes to investigate a large number of users in order to identify one malicious actor. The EU will therefore encourage the uptake of the new protocol (as it allows the allocation of a single user per IP address, thus bringing clear benefits to law enforcement and cybersecurity investigations. As a first step to encourage this action, the Commission will mainstream the requirement to move to IPv6 throughout its policies, including requirements in procurement, project, and research funding, as well as supporting the necessary training materials. In addition, Member States should consider voluntary agreements with Internet Service Providers to drive the adoption of IPv6. More generally, online accountability should be further promoted. This further means that the promotion of measures to prevent the abuse of domain names for the distribution of unsolicited messages or phishing attacks is also of high importance. To this end, the Commission will work to improve the functioning of and the availability and accuracy of information in the domain name and IP systems in line with the efforts of the Internet Corporation for Assigned Names and Numbers.

Steps forward- Key actions

1. Full implementation of the Directive on the Security of Network and Information Systems;
2. Adoption by the European Parliament and the Council of the Regulation setting out a new mandate for ENISA and a European framework for certification[252];
3. A joint Commission/industry initiative as to define a "duty of care" principle for reducing product/software vulnerabilities and promoting "security by design";
4. Implementation of the blueprint for cross-border major incident response;
5. Launch of an impact assessment to study the possibility for a Commission proposal in 2018 to set up a network of Cybersecurity competence centres and a European Cybersecurity Research and Competence Centre, building on an immediate pilot phase;
6. Support Member States in identifying areas where common cybersecurity projects could be considered for support by the European Defence Fund;
7. An EU-wide one-stop-shop to help victims of cyber attacks, providing information on latest threats and bringing together practical advice and cybersecurity tools;
8. Action by Member States to mainstream cybersecurity into skills programmes, e-government, and awareness campaigns.

Action by industry to step up cybersecurity-related training for their staff and adopt a "security by design" approach for their products, services, and processes.

Conclusions

EU cyber preparedness is central to both the Digital Single Market and our Security and Defence Union. Enhancing European cybersecurity and addressing threats to civilian and military targets is a must.

The Commission calls on the Member States to commit how they intend to act in areas where they have the primary responsibility. This should include strengthening cybersecurity by:

1. Applying the same rules to public administrations, given the role they play in society and the economy as a whole;
2. Providing cybersecurity-related training in public administration;

[252] Unless otherwise stated, proposals in this Communication are budgetary neutral. Any initiative having budgetary implications will duly follow the annual budget procedures and cannot prejudge the next Multi-Annual Financial Framework post-2020.

3. Prioritising cyber-awareness in information campaigns and including cybersecurity as part of academic and vocational training curricula;
4. Using initiatives on the "Permanent Structured Cooperation" (PESCO) and the European Defence Fund to support the development of cyber defence projects.

This Joint Communication has set out the scale of the challenge and the range of measures that the EU can undertake. There arises the necessity to enhance that Europe will be resilient, managing also to protect its people effectively by anticipating possible cybersecurity incidents and building strong protection in its structures and behaviour, by recovering quickly from any cyber-attacks, and by deterring the organisations and persons responsible. This Communication puts forward targeted measures which will further strengthen the EU's cybersecurity structures and capabilities in a coordinated manner, reaching also the full cooperation of the Member States and the different EU structures concerned, as well as respecting their competencies and responsibilities. Its implementation will provide a clear demonstration that both the EU and the member states will work together to face the upcoming challenges faced by Europe today[253].

6.5 Information field analyses related to strategic events (LKA).

General information about the subcase

Disinformation and related cyber incidents are often used for interference in democratic elections. Hence, the punitive consequences of disinformation depend on national laws (criminal, electoral, media regulation or no regulation at all), the monitoring of ongoing disinformation campaigns helps to counter it and prevent future interference. Also, if there is no significant interference during elections, it might be that there is another more important target for foreign power at the moment. Therefore, not only the national, but also the international context is important in interpreting the results of disinformation monitoring.

The analyses of Latvian municipal elections on 2021 were made using DebunkEU.org AI tool. The methodology of this tool is based on a tiered approach: 1) source identification; 2) content assessment; 3) circumstances assessment. Domains known for publishing harmful content analysed by DebunkEU.org are categorised using the source classification method: languages, region, traffic, type of media, type of ownership, etc. The task of DebunkEU org. The AI tool is to spot and redistrict the most harmful stories, which are then analysed by the human analytics.

The content analysis of communications about the Latvian municipal elections, which were categorised separately in three objects – electoral process, election management body/procedures and participants of the elections – at the same time divided into three audiences of interest both in Latvia and abroad:

1. Latvian language - domestic readers in Latvian. Suspicious Latvian language media were analysed (pietiek.com, brivibasplatforma.lv, etc.).
2. Russian language - Russian speaking part of Latvian society, Russian diasporas living in other post-Soviet space countries, Russian language users where Russian is a primary language (Russia, Belarus). Hostile Russian language media (gazeta.ru, vpk-news.ru, riafan.ru, 3mv.ru, rossaprimavera.ru, vesti.ru, ntv.ru etc.) and media outlets in Latvia dedicated to the Russian-speaking part of the society (lv.sputniknews.ru, mklat.lv etc)
3. English language, English-speaking countries and/or international organisations, etc. Foreign-facing media outlets in English (rt.com, tass.com etc.) were analysed.

The result of the analysis was presented at the T-SHARK meeting.

[253] European ICT Law Texts, Cases, Materials, https://ictlaw.weebly.com/uploads/3/7/8/6/37865075/cyberlawreader2018.pdf

Relevant legal regulation for the sub-case analyses

1. Art. 8, EHRC;
2. Art. 7, CFR;
3. GDPR;
4. National laws on personal data protection for law enforcement, national security, and defence purposes;
5. National laws on criminal procedures.

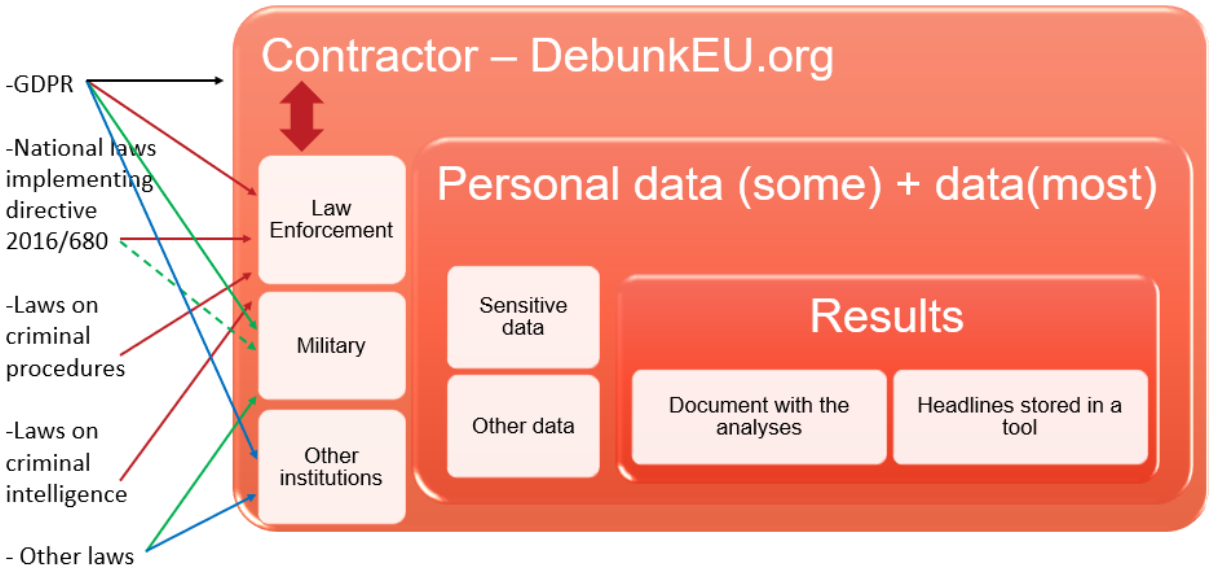


Figure 5: DebunEU.org legal compliance

Legal Analyses

DebunkEU.org AI tool analyses publicly available content - online media articles. While performing analysis, mainly not personal data is collected (data about information source, context surrounding the appearance of information, etc). But the personal data might also be processed as part of the content of the articles or posts (for example, photos, quotes, personal opinions made publicly available), IP addresses if the author of a post is a natural person, not an entity. The DebunkEU.org AI tool does not store any personal data itself, but it might use it during the analysis and it might be included in reports of analysis carried out. DebunkEU.org stores only the headlines of articles and references.

Art. 8 of ECHR and Art. 7 of CFR enshrines the right to privacy and personal data protection being not absolute. However, neither the limitations of the right to privacy and personal data protection, entitled in ECHR and CFR, nor the scope of GDPR regulation and the notion of personal data exclude publicly available personal data from the personal data protection regulation. Therefore, publicly available data is personal data despite its publicity. The legitimate basis on personal data processing by DebunkEU.org depends on the purpose of personal data collection and it differs depending on the client of the entity running DEbunkEU.org tool. So, the legitimate basis for an entity to use DebunkEU.org tool is a contract with a client (Art. 6 (1 (c) or (e) of GDPR). Due to the contractual relationship an entity running DebunkEU.org tool becomes a processor of personal data and the client a controller. Depending on national systems which are overviewed in Chapter 3 of this deliverable, there might be few types of controllers (task forces): 1) law enforcement institution; 2) military or national defence institution; 3) public or civil institutions. The activities of mentioned task forces dealing with the same issue – disinformation – are regulated by different laws. Therefore, the purpose of personal data processing (law enforcement, national defence, media regulation, election

monitoring or other) also determines if GDPR or other national laws apply for data controller[254]. Different legal personal data protection regimes apply for different DebunkEU.org clients. Not only the processor (an entity owning DebunkEU.org tool), but also the controller has to enter the contact legally, i. e. has to have a legitimate basis according to the laws to process personal data for the fight against disinformation purposes.

Customer/ data controller - law enforcement institution. The main laws regulating processing of personal data for law enforcement purposes are national laws on criminal procedures, national laws on criminal intelligence, and national laws implementing Directive 2016/680[255] (see. Figure 5). The laws implementing Directive 2016/680 set out the principles of lawful personal data processing. However, national laws on criminal procedures and laws on criminal intelligence impose a set of rules governing the series of proceedings of personal data collection in cyberspace. Despite recent case law rulings on treating content of electronic communication and meta data equally as personal data[256]countries still have a distinction in criminal procedure laws between these two categories of personal data. The content of communication in cyberspace is considered to have a higher level of intrusion into privacy and higher legal protection. Consequently, judicial authorization is required for the collection and processing of the content of the communication. However, personal data which are metadata might be collected with the authorization of the Attorney General or with no authorization at all. Also in some cases collection of metadata (which is personal data) is interpreted by law enforcement institutions in a way it falls under their right to collect information in general[257]. As long as national laws have loopholes in electronic surveillance laws, there will be a possibility to choose the most appropriate legal basis to enter into the contract with an entity using DebunkEU.org tool.

Customer/data controller – military or national defence institution. Disinformation can be enacted as a threat to national security. For example, Lithuanian Military Strategy[258], White Book on Defence Policy[259] and proposed National Security Strategy[260] foresee disinformation as a threat to national security. National security and defence are the areas where EU laws are not applicable. Therefore, GDPR only applies for defence purposes not related to personal data processing. The national laws transposing Directive 2016/680 generally do not apply as well. However, some member states expanded it to the areas of defence and national security as well[261]. The laws regulating the procedures of collecting personal data for national defence and security purposes differ, as might differ the scope of personal data. However, Art. 8 of the ECHR enshrining the right to privacy also applies to the area of national security and defence. The nature of disinformation imposes that the personal data of non-residents of the country might often be processed. Therefore, all the Member States that ratified the convention should ensure the right to privacy not only to their inhabitants. For example, Germany's Constitutional Court ruled that processing foreign people's metadata for national security purposes without authorization infringes the right to privacy. However, the national law imposed procedures of personal data - metadata processing - are less regulated than the processing of other types of personal data.

[254] GDPR does not apply for data processing for the purposes of national security, defence and law enforcement (Art 2 of GDPR).
[255] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
[256] "Briefing Note: Why Communications Data (Metadata) Matter", Big Brother Watch, https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf .
[257] Sigutė Stankevičiūtė, doctoral dissertation "Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas", 2020, Vilnius.
[258] Lietuvos Respublikos karinė strategija, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2016 m. kovo 17 d. įsakymu V-252.
[259] Lietuvos gynybos politikos Baltoji knyga, 2017.
[260] Pasiūlymas dėl Nacionalinio saugumo strategijos, 2021.
[261] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Since there is no unified approach about disinformation being a threat to national security in the EU, therefore, the legality of each case of using DebunkEU.org AI tool should be analysed individually.

However, the exemption of GDPR applies to the competent authority, but not to DebunkEU.org, which is a private company. Therefore, the contract between the competent authority and DebunkEU.org is required. The legal basis for DebunkEU.org to process personal data under GDPR is the legitimate interest or legal obligation (Art. 6 of GDPR) of the contractor (competent authority), which might be a military, law enforcement, or other relevant institution.

Customer/data controller – public or civil organisation. Public or civil organisations are subject to GDPR regulations. Therefore, each organisation has to have a legitimate basis in accordance with GDPR to process personal data. The role in fighting against disinformation should be entitled in the articles of association, bylaws or other national level documents. So the legal basis for collecting personal data is the legitimate interest or legal obligation (Art. 6 of GDPR).

Problems

The data controller – the client - might not consider that any personal data would be processed. Therefore, they might not apply for authorization even though it is required by national laws or not apply any of the data protection laws. Consequently, the admissibility of evidence collected could be questioned in court (if a client is a law enforcement institution) or a national person could claim damages (if the controller is a defence or public institution).

Recommendation

An entity running DebunkEu.org should provide written information about the possibility of personal data being processed to their potential client.

6.6 Anticipation of the cyber-physical attack on transport CII (INDRA)

General information about the subcase

Critical Information Infrastructure plays a vital role for the well-functioning of society and economy by affecting infrastructures, which could have cascading effects on a large part of the population. Moreover, cyberattacks on critical infrastructure have become increasingly more complex and more disruptive, causing systems to shut down, disrupting operations, or simply allowing attackers to remotely control affected systems[262]. Cyberattacks on critical infrastructures can also have a significant economic impact, especially when targeted in conflict between nations. Securing these systems is not a matter of fully reverting to physical access, but a matter of understanding how internet-connected control systems work, how they are configured, and how they are accessed[263]. Visibility and management are the key to improving security, but security and IT professionals must be aware of the risks and establish security controls to reduce the impact of a potential cyberattack and increase the cost of attack for threat actors[264].

This sub-case scenario will try to take advantage of new security challenges that arise from the digitalization era. In this context, one of them is the case of roads as a critical transport infrastructure. The participants will conduct three main activities, which will define the sub-case demonstration stages: First, digitalization of the key cyber-physical asset of the covered CII infrastructure will be

[262] The Importance of Critical Infrastructure Security, https://www.cipsec.eu/content/importance-critical-infrastructure-security
[263] Ibid.
[264] Protecting Critical Infrastructure, https://www.cybersecurityintelligence.com/blog/protecting-critical-infrastructure-5698.html

instantiated in a secure and isolated environment, where automatic or human-driven tests shall allow discovering specific Cyber Threat Intelligence like potential attack surfaces, cyber-to-physical propagations, and evaluation of simulation-driven if-then scenarios. At the second stage, the gathered information will serve for guiding the custom hardening of the operational environment, definition of high-level safety/security policies, and cataloguing potential courses of action. Finally, based on the outputs of the previous stages, capabilities for facilitating the acquisition of situational awareness (e.g. human-centric visualisations, human-in-the-loop simulations) and its projection at different time horizons will be conducted, which shall support reactive/proactive decision making (e.g. anticipation of next stages of cyber kill chains)[265].

Following this, INDRA demo sub-case focuses on detecting ongoing cyber-attacks to a particular segment of a road infrastructure. A risk-oriented assessment has been performed and assets have been prioritised. Since the demo subcase is running on real infrastructure, IT components cannot be updated so easily, which means that IT security must be 'plugged' in some way into the system. Finally, passive data gathering sensors have been incorporated into the target system architecture.

The data that are processed are the interaction of external sources with the platform in charge of managing the transport critical infrastructure. A data sample is, if a detected anomaly into communication queues between target infrastructure subsystems.

Relevant legal regulation for the sub-case analyses

According to the answers provided by NASK, the types of data related to the subcase were as follows:

Internal Components

- Signalling
- Video Surveillance
- Traffic Measurement
- Alerts in Message Panel Queues
- Traffic alerts
- Incident alerts
- IPs from where external sources try to perform malicious actions against the critical infrastructure platform of transport.

Taking into account the application of the Law Enforcement Directive, LED (EU 2016/680[266]) notably processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, falls under the directive EU 2016/680[267].

Having also regard to Article 70 (1e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by

[265] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

[266] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[267] Guidelines 3/2019 on processing of personal data through video devices, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

the Decision of the EEA joint Committee No 154/2018 [268]on 6 July 2018, the European Data Protection Board has adopted guideline 3/2019 on processing of personal data through video devices.

In accordance with GDPR, every legal ground under Article 6 (1) can provide a legal basis for processing video surveillance data. For example, Article 6 (1) (c) applies, where national law stipulates an obligation to video surveillance[269]. However in practice, the provisions most likely to be used are

- Article 6 (1) (f) (legitimate interest).
- Article 6 (1) (e) (necessity to perform a task carried out in the public interest or in the exercise of official authority), whether in rather exceptional cases Article 6 (1) (a) (consent) might be used as a legal basis by the controller.

Steps forward

Taking into account the issues arising from the cyber threats, it is noticed that they refer to some strategies, which are followed in terms of an operation in order to deal with the problems that occurred. In these terms, the strategies to address the proposed threats are divided into those that concern operators and those relevant to the countries involved.

1. for Operators
    - Define a risk management framework
    - Build and test emergency plans
    - Training and education
    - Supply chain security
    - Information Sharing and Cooperation
    - Legal Compliance
    - Continuous monitoring and assessment of cybersecurity posture
2. for countries
    - Institutional architecture
    - National Risk Assessment
    - Identification of Critical Information Infrastructure
    - Strategies, policy, regulation, and standards
    - Public- private cooperation
    - Education and capacity building
    - Development of a Trusted Market
    - National Crisis Management
    - Monitoring and improvement[270].

[268] Decision of the EEA Joint Committee No 154/2018 amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (containing the List Provided for in Article 101) to the EEA Agreement) https://www.dataguidance.com/legal-research/decision-eea-joint-committee-no-1542018

[269] Guidelines 3/2019 on processing of personal data through video devices, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf

[270] CIIP Overview Introduction to Critical Information Infrastructure Protection, https://docplayer.net/199732000-Ciip-overview-introduction-to-critical-information-infrastructure-protection.html

Definition of a risk management framework

This goal develops a continuous and repeatable methodology to identify, assess and respond to cybersecurity risks. In addition to that, organisations can also determine their risk tolerance, thus the acceptable level of risk to achieve their supply and organizational goals, and are able to prioritize remediations and make informed decisions about cybersecurity investments.

Legal Compliance

At this stage, the achievement of legal compliance is of great importance in order to ensure that operators meet critical security standards identified by national decision makers. Regarding intellectual property issues and more specifically our question included in the questionnaire with reference: 'Indicate *whether the license of the software asset that is or will be produced through the subcase is going to be proprietary or Open Source'* the relevant answer provided was that the HORUS license is proprietary. Furthermore, the INDRA monitoring solution is based on open software, while in future iterations may use commercial linq software. In this case, the licensed iterations will comply with European legislation regarding intellectual property assets.

Continuous monitoring & assessment of cybersecurity posture

The digital risk landscape is constantly evolving and needs to build repeatable processes to monitor and assess the level of cybersecurity maturity on an ongoing basis. In these terms, the assessment should consider the risk-related adequacy of processes, people, and technology, to identify substantial gaps in cybersecurity and determine appropriate remedies to resolve weaknesses.

Solutions - Future proposals

A shift in mindset in the manner of cybersecurity must be addressed to look beyond technical tools and manage to adopt a new cyber defence strategy. For this reason, it is of great importance to conduct training and vulnerability assessment in order to build robust national policies and strategies. In these terms, it is needed to design sector-specific resources and initiative, to expand information sharing and collaboration, and cooperate in general with agencies on a national, regional, and international level.

6.7 Sharing of Machine Learning Models (CESNET)

General information about the subcase

The envisioned solution evolves the traditional approach to the detection and sharing of indicators of compromise. The aim is to broaden the scope of sharing data between multiple organisations supporting privacy (e.g. non-privacy-sensitive features extracted from raw data, anonymised monitoring data, encrypted features, sharing only query results, etc.). Essentially, the intention is not to share the raw data, but rather pre-processed data up to the classification models. The indicators are being trained on each partner's internal datasets without sharing the data but sharing the resulting indicator of compromise. The same indicator is then, in turn, run on another partner's dataset.

Sharing of classification models allows to train the classification models in a distributed way. In addition, it provides a new way of looking at an indicator of compromise. Similarly to a hash of a file, which classifies the file to be either malware or not, we can use classification model (e.g. a neural network) and use it to decide whether behaviour of an IP address is benign or not. In both cases, the sharing for distributed learning and the new IoC, the data model is the same.

Relevant legal regulation for the sub-case analyses

As the solution does not require sharing of data but an IoC which is trained on internal datasets, the relevant EU regulation is GDPR and it will be applied to the extent of an internal data protection for partners involved in the task. The model uses a privacy-by-design approach in developing the IoC without compromising the data by sharing it between partners. This type of approach reduces the surface of vulnerability of the data used and better ensures the protection of it as the data controller is minimised by a single entity.

The element that is being shared is the IoC itself, which raises the question of shared intellectual property. For this purpose, an agreement between partners in regard to potential exploitation, both commercial and non-commercial, should be agreed to avoid future litigation.

As a recommendation for this specific subcase, it has to be ensured that either no personal data are processed, personal data is anonymized, and if not, that GDPR obligations are fulfilled. These obligations can be very burdensome, and a decision has to be taken if efforts are invested in full GDPR compliance or technical avoidance mechanisms such as anonymization of the data. If the data can, for instance, be anonymized, this should be done at an early stage since the anonymization unburdens legal compliance requirements. Having a proper data collection policy is of utmost importance here and should be drafted on a case-by-case basis for every deployment of the tool.

Furthermore, as machine learning processes are being used by the subcase, a clear policy should be developed on what kind of data is fed to these algorithms. Especially, ethical and societal requirements should be respected and considered by this policy. The creation of a clear data management plan at the beginning of the project can be of use here.

6.8 A specialized Virtual Control Room for protection of a Critical Infrastructure (LEO)

General information about the subcase

This subcase aims to propose a Virtual Control Room that provides situational awareness for the cyber/ physical protection of critical infrastructures, providing operators with a virtual interface. The prototype will be demonstrated by considering as critical infrastructure the Leonardo High-Performance Computer (HPC) and related assets, with connection to the video camera system present at Chieti premises. The core system is based on an OSINT platform that will attempt to identify vulnerabilities and malware related to the protected critical asset. The information will be captured in real time and it will be available to the operator in the virtual environment for analysis. Furthermore, information on the safety status of protected assets and information from SCADA control systems will be shown in real-time, through virtual video walls. In particular, it will be possible to monitor all the alerts coming from the perimeter security systems (Firewalls, SIEM). A Decision Support function will be used to propose operators, actions to manage cyber-attacks/physical intrusions. To summarise, the main capabilities of the Visual Control Room will cover the mapping and monitoring of the situations, comprehension of the situation, projection the effects that different actions may have, and finally, support on the decisions and the actions that must be taken[271].

Relevant legal regulation for the sub-case analyses

Since only fake data are used for sub cases and no personal data is processed, GDPR is not applicable. Therefore, the legal issues could be related to access rights management with 1) service providers and 2) users. The owner of the subcase confirmed that access rights issues are dealt with individually by each service provider. Also, the Virtual Control Room is accessible only on a physical machine which is located in the Leonardo Research and Development Laboratory with limited access

[271] SPARTA D4.1 Cybersecurity threat intelligence common data model, https://www.sparta.eu/assets/deliverables/SPARTA-D4.1-Cybersecurity-threat-intelligence-common-data-model-PU-M18.pdf

(username/password). It means that only authorized personnel who signed confidentiality agreements can access it. Therefore, there are no legal issues while Virtual Control Room is used only for research purposes, and no personal data is involved. However, if Virtual Control Room will be used in real life operations, personal data protection impact assessment and related legal regulation on personal data protection should be considered. Also, end users' access rights management should be considered in a way that different end users can be legally entitled to different scope of information to be accessed.

Chapter 7 Concluding Remarks

1. The legal measures against disinformation differ in EU member states. It could be regulated by electoral, media or criminal law, and the regulation itself is different. The diversity of legal regulation of disinformation makes it difficult to fight against at the EU level.
2. Only natural persons could be charged with crimes related to disinformation, despite the majority of cases being related to legal persons. Thus, making it difficult to address the actual threat.
3. An assessment of the impact of cyber threats on critical infrastructure is proposed both at the EU and at the national level with the aim of collecting more evidence from several different sources:
   3.1. At the present time, a study is ongoing that will inform the impact assessment process. It will also use a combination of qualitative and quantitative methodologies, with the aim of collecting relevant data and contextual information, which is necessary for the analysis. The study will take into account the entire scope of the EPCIP, including the ECI Directive, as well as other CIP-relevant initiatives taken at European level on both a sectoral and cross-sectoral basis in order input through various consultation activities to be collected.
   3.2. Following that, a legislative proposal can take place based on a number of targeted consultations with a wide range of stakeholders, including competent Member States authorities, operators of critical infrastructures and other industry stakeholders, international organisations, as well as academia and think-tank representatives. The consultation activities would rather involve interviews, surveys, and workshops. The following consultation activities can be planned:
   3.3. Web-based survey with relevant authorities in member states (completed), followed by in-depth interviews with representatives of member states.
   3.4. Interviews with relevant international organisations; representatives of EU institutions, and representatives of academia and think tanks.
   3.5. Consultative workshops with Member States, critical infrastructure operators and national and European associations of operators in different sectors focused on validation of problem definition / baseline scenario; and on definition of possible policy measures.
4. The main obstacle in universal implementation of the proposed DSos backscatter TRaffic Detection models stems from the Member States' national laws and whether or not low-intensity attack on an individual IP or computer falls under national definition of cybercrime. The law enforcement directive grants the permission to process data for the purposes of detecting ongoing crime for criminal offences. Therefore, Member State national legislation does not accept low intensity DDoS as a cybercrime, and the module could not be implemented in detecting low intensity DDoS attacks. However, this does not restrict the implementation of the module in detecting significant interferences resulting from DDoS attacks. National regulations need to be observed very carefully in order to implement the technology in different Member States, or a consideration of adopting legislation that recognises DDoS attacks on an individual IP or computer should be recognised.
5. A shift in mindset in the manner of cybersecurity must be addressed to look beyond technical tools and manage to adopt a new cyber defence strategy. For this reason, it is of great importance to conduct training and vulnerability assessment in order to build robust national policies and strategies. In these terms, it is needed to design sector-specific resources and initiative, to expand information sharing and collaboration, and cooperate in general with agencies on a national, regional, and international level.

Chapter 8 List of abbreviations

Abbreviations	Translation
GDPR	General Data Protection Regulation
ECHR	European Convention on Human Rights
CFR	Charter of Fundamental Rights of the European Union
Law Enforcement Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with respect to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing the Council Framework Decision 2008/977/JHA
EU	The European Union

Chapter 9 Bibliography

1. ‘Briefing Note: Why Communications Data (Metadata) Matter‘, Big Brother Watch, https://www.bigbrotherwatch.org.uk/wp-content/uploads/2014/07/Communications-Data-Briefing.pdf .

2. ‘Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States: - 2021 update’, April 2021, https://www.sipotra.it/wp-content/uploads/2021/05/Disinformation-and-propaganda-impact-on-the-functioning-of-the-rule-of-law-and-democratic-processes-in-the-EU-and-its-Member-States-2021-update.pdf

3. ‘Measuring the reach of "fake news" and online disinformation in Europe’, https://reutersinstitute.politics.ox.ac.uk/our-research/measuring-reach-fake-news-and-online-disinformation-europe

4. ‘SJ questiona constitucionalidade do artigo 6.º da carta dos direitos digitais’, Sindicato dos Jornalistas, 9 June 2021, https://jornalistas.eu/sj-questiona-constitucionalidade-do-artigo-6-o-da-carta-dos-direitos-digitais/

5. ‘Source alerts can reduce the harms of foreign disinformation’, https://misinforeview.hks.harvard.edu/article/source-alerts-can-reduce-the-harms-of-foreign-disinformation/

6. ‘Spain: New law threatens internet freedoms’, 18 December 2019, EDRI, https://edri.org/our-work/spain-new-law-threatens-internet-freedoms/

7. ‘Spain: The Royal Decree-Law 14/2019 threatens freedom of expression‘, Article 19, 11 February 2020, https://www.article19.org/resources/spain-ministerial-order-on-disinformation-should-favour-multi-stakeholder-approach/

8. ‘Who calls the shots on fake news? The minefield of countering lies in the Baltics’, lrt.lt, 29 May 2021, https://www.lrt.lt/en/news-in-english/19/1418424/who-calls-the-shots-on-fake-news-the-minefield-of-countering-lies-in-the-baltics

9. Act 300/2005 Coll. of 20 May 2005, Criminal Code of Slovakia, https://www.legislationline.org/download/id/3763/file/Slovakia_CC_2005_en.pdf

10. Act C of 2012 on the Criminal Code, promulgated on 13 July 2012, https://www.legislationline.org/download/id/5619/file/HUngary_Criminal_Code_of_2012_en.pdf

11. Act No. 269 amending the Penal Code of 26/03/2019, https://www.retsinformation.dk/eli/lta/2019/269

12. Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act), https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=433744569E4AA4A03CED91951420A4DA.2_cid297?__blob=publicationFile&v=2

13. AEJ Bulgaria, Criticizing Anti-Pandemic Measures and Policies Cannot Be a Ground for Prosecution, 14 April 2020, https://aej-bulgaria.org/en/criticizing-anti-pandemic-measures-and-policies-cannot-be-a-ground-for-prosecution/

14. Amendments to the Penal Code, the Code of Criminal Procedure and other provisions, https://collab.lawspot.gr/sites/default/files/mashup/feka/2021/fek-215-2021.pdf

15. Amnesty International, Høringsnotat, 11 October 2018 https://amnesty.dk/wp-content/uploads/media/5012/amnesty-international-hoeringssvar-om-hjaelp-til-fremmede-efterretningstjenester.pdf

16. Anforderungen an eine kohärente Regulierung der Cybersicherheit, https://www.bitkom.org/sites/default/files/2019-06/20190606_anforderungen_an_eine_koharante_regulierung_der_cybersicherheit.pdf

17. BalkanInsight, Romania's State of Emergency Raises Media Freedom Concerns, by Marcel Gascon Barbera, https://balkaninsight.com/2020/03/31/romanias-state-of-emergency-raises-media-freedom-concerns/

18. Baumann, M.. 'Propaganda Fights' and 'Disinformation Campaigns': the discourse on information warfare in Russia-West relations. Contemporary politics, 26(3), 288-307.

19. Bitkom, *Anforderungen an eine kohärente Regulierung der Cybersicherheit*, June 18th 2019,

20. Blocman, A. 'Laws to combat manipulation of information finally adopted', European Audiovisual Observatory, https://merlin.obs.coe.int/article/8446

21. Brattberg, E., & Maurer, T. (2018). Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks (Vol. 23). Washington, DC: Carnegie Endowment for International Peace.

22. Brocardi.it, https://www.brocardi.it/codice-penale/libro-terzo/titolo-i/capo-i/sezione-i/art656.html

23. Brown, I., Marsden, C. T., Lee, J., & Veale, M. Cybersecurity for elections: A Commonwealth guide on best practice.

24. C-622/17, Baltic Media Alliance v. Lietuvos radijo [2019] ECLI:EU:C:2019:566.

25. Camera dei Deputati, Modifica dell'articolo 656 del codice penale e altre disposizioni in materia di pubblicazione o diffusione di notizie false, esagerate o tendenziose, presentata il 15 giugno 2017, https://www.camera.it/leg17/995?sezione=documenti&tipoDoc=lavori_testo_pdl&idLegislatura=17&codice=17PDL0053180

26. Cassazione penale, Sez. I, sentenza n. 9475 del 7 novembre 1996

27. Changes of the law, https://www.lexology.com/library/detail.aspx?g=a2b6a2dd-f23a-43fe-a190-87177e5f66e3

28. Code électoral, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070239/LEGISCTA000006148461/?anchor=LEGIARTI000006353232#LEGIARTI000006353232

29. Convention on Cybercrime (ETS No. 185) https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

30. Convention on Cybercrime, https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

31. Council of Europe report, Information Disorder: Toward an interdisciplinary framework for research and policy making, 2017, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

32. Council of Europe, Convention on Cybercrime, 23 November 2001, CETS No.185.

33. Criminal Code of Cyprus (text amended in 2021), http://www.cylaw.org/nomoi/enop/ind/0_154/section-sc538de4e7-f17f-4668-a2b7-34f90b34ac1e.html

34. Criminal Code of Cyprus of 1959, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=NIM:289553

35. Criminal Code of Italy, https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-penale

36. Criminal Code of Malta, https://justice.gov.mt/en/pcac/Documents/Criminal%20code.pdf

37. Criminal Code of the Czech Republic, https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf

38. Criminal Code of the Czech Republic, https://www.legislationline.org/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf

39. Criminal Code of the Republic of Austria, https://www.legislationline.org/download/id/8548/file/Austria_CC_1974_am122019_de.pdf

40. Criminal Code, https://www.finlex.fi/en/laki/kaannokset/1889/en18890039_19951010.pdf

41. Croatian Criminal Code No. 110 of October 21, 1997, http://www.vsrh.hr/CustomPages/Static/HRV/Files/Legislation__Criminal-Code.pdf

42. Cynthia Donoghue and Howard Womerseley Smith, *Technology Law Dispatch: EU Cybersecurity Act gets the green light, June 11th 2019,*

43. Décision n° 2018-773 DC du 20 décembre 2018, https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm#:~:text=LE%20CONSEIL%20CONSTITUTIONNEL%20A%20%C3%89T%C3%89,21%20novembre%202018%2C%20par%20MM.

44. Decision of the EEA Joint Committee No 154/2018 amending Annex XI (Electronic Communication, Audiovisual Services and Information Society) and Protocol 37 (containing the List Provided for in Article 101) to the EEA Agreement) https://www.dataguidance.com/legal-research/decision-eea-joint-committee-no-1542018

45. Decree on the extension of the state of emergency in the territory of Romani, https://rm.coe.int/16809e375e,

46. Décret n° 64-1086 du 27 octobre 1964 portant révision du code électoral, https://www.legifrance.gouv.fr/download/securePrint?token=@ZXug0XOZQC!6dScf4z$

47. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016.

48. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union

49. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the

execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

50. Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crimehttps://eclan.eu/en/eu-legislatory/directive-eu-2016-681-of-the-european-parliament-and-of-the-council-of-27-april-2016-on-the-use-of-passenger-name-record-pnr-data-for-the-prevention-detection-investigation-and-prosecution-of-terrorist-offences-and-serious-crime

51. Directive 2002/58/EC of the European Parliament and of the Council, https://www.legislation.gov.uk/id/eudr/2002/58

52. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data

53. Directive 2008/114 - Identification and designation of European critical infrastructures and the assessment of the need to improve their protection, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vitgbgipfogy

54. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against

55. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems.

56. Durach, F., Bârgăoanu, A., & Nastasiu, C. (2020). Tackling disinformation: EU regulation of the digital space. Romanian Journal of European Affairs, 20(1).

57. ECPMF, 'Hungary's two pandemics: COVID-19 and attacks on media freedom', 17 June 2020, https://www.ecpmf.eu/hungarys-two-pandemics-covid-19-and-attacks-on-media-freedom/

58. Eighth progress report towards an effective and genuine Security Union of 29 June 2017, COM (2017) 354 final.

59. eng.lsm.lv, 'Man charged with hooliganism for running fake Latvian news websites', https://eng.lsm.lv/article/society/crime/man-charged-with-hooliganism-for-running-fake-latvian-news-websites.a325793/,

60. ENISA and a new cybersecurity act, https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI(2017)614643_EN.pdf .

61. ERGA, 'Notions of disinformation and related concepts, 2021, p. 10 https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf

62. EU Global Strategy, http://europa.eu/globalstrategy/.

63. European Centre for Press and Media Freedom, Greece: Justice Ministry must withdraw amendment on 'false news', 12 October 2021, https://www.ecpmf.eu/greece-justice-ministry-must-withdraw-amendment-on-false-news/

64. European Commission, *DSM Fact Sheet: EU Cybersecurity Act*.

65. European Commission, *Questions and answers – EU Cybersecurity,* June 26th 2019,

66. European Commission, Report from the Commission to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Brussels, 13.9.2017 COM (2017) 474 final, p.4.

67. European Commission, *Shaping the Digital Single Market,*

68. European Commission, *Strengthening Europe's Cyber resilience system and fostering a competitive and innovative cybersecurity industry*, July 5th 2019,

69. European Council conclusions, 22-23/06/2017, http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

70. European Court of Human Rights (Plenary), *Klass and others v. Germany*, 6th. of September 1978, application no. n. 5029/1971.

71. European Court of Human Rights, *S and Marper v. United Kingdom,* December 4th 2008, application no. 30562/04 and 30566/04.

72. European Parlament, The impact of disinformation on democratic processes and human rights in the world,2021 https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf.

73. European Parliament Briefing, *ENISA and a new cybersecurity act*, July 5th 2019,

74. European Programme for Critical Infrastructure Protection https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33260

75. European Union, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 2000/0189/COD.

76. Filipec, O. (2019) Towards a Disinformation Resilient Society? The Experience of the Czech Republic, Cosmopolitan Civil Societies: an Interdisciplinary Journal, 11 (1), p. 10, https://doi.org/10.5130/ccs.v11.i1.6065

77. France: Statute of Limitations Extended for Criminal Offenses, https://www.loc.gov/item/global-legal-monitor/2017-03-21/france-statute-of-limitations-extended-for-criminal-offenses/

78. Funke, D., and Flamini, D., 'A guide to anti-misinformation actions around the world', Poynter, https://www.poynter.org/ifcn/anti-misinformation-actions/

79. German Constitutional Court stops mass surveillance abroad, https://edri.org/our-work/german-constitutional-court-stops-mass-surveillance-abroad/.

80. German Criminal Code, https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1441

81. Gotev, G. Rotaru, S. 'Romania shuts down websites with fake COVID-19 news', https://www.euractiv.com/section/all/short_news/romania-shuts-down-websites-with-fake-covid-19-news/,

82. Greek Penal Code https://collab.lawspot.gr/sites/default/files/mashup/feka/2021/fek-215-2021.pdf

83. Grosseck, G., Malita, L. (2020). Insights from Romania's Reaction to Coronavirus Infodemic. towardsan Educational Approach. Logos Universality Mentality Education Novelty: Social Sciences, 9(1), 119-138. doi: 10.18662/lumenss/9.1/38, https://lumenpublishing.com/journals/index.php/lumenss/article/view/3136/pdf, p. 128.

84. Győry, C. (2020) *Fighting Fake News or Fighting Inconvenient Truths?: On the Amended Hungarian Crime of Scaremongering, VerfBlog,* 2020/4/11, https://verfassungsblog.de/fighting-fake-news-or-fighting-inconvenient-truths/, DOI: 10.17176/20200411-152518-0.

85. Heldt, A. 'Germany is amending its online speech act NetzDG... but not only that', Internet Policy Review, https://policyreview.info/articles/news/germany-amending-its-online-speech-act-netzdg-not-only/1464

86. HINA, 'Most Croatian Media Without Fake News on Pandemic', 11 October 2020, https://www.total-croatia-news.com/news/47317-most-croatian-media-without-fake-news-on-pandemic

87. HINA, 'Most Croatian Media Without Fake News on Pandemic', 11 October 2020, https://www.total-croatia-news.com/news/47317-most-croatian-media-without-fake-news-on-pandemic

88. Hoboken, J., Fathaigh, Ó R. Regulating Disinformation in Europe: Implications for Speech and Privacy, 6 UC Irvine Journal of International, Transnational, and Comparative Law, 9, https://scholarship.law.uci.edu/cgi/viewcontent.cgi?article=1041&context=ucijil, p. 20

89. How false information spreads, https://www.bbc.co.uk/bitesize/articles/zcr8r2p

90. Human Rights Watch, 'Greece: Alleged 'Fake News' Made a Crime', https://www.hrw.org/news/2021/11/17/greece-alleged-fake-news-made-crime,

91. Hungary's Two Pandemics, https://www.ecpmf.eu/wp-content/uploads/2020/06/Legal-opinion-Hungary_2020.pdf

92. ICT process: "A set of activities performed to design, develop, deliver or maintain an ICT product or service" (CSA Article 2).

93. Indaco lege, https://lege5.ro/gratuit/gezdmnrzgi/art-404-comunicarea-de-informatii-false-codul-penal?dp=gqytsojwge3te

94. Information Commissioner's Office, *Right to Data Protability at a glance.*

95. Ireton, C., Posetti, J., 'Journalism, fake news & disinformation: handbook for journalism education and training', https://unesdoc.unesco.org/ark:/48223/pf0000265552,

96. Joint Communication to the European Parliament and the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europet .

97. Judgment of the General Court (First Chamber, Extended Composition) of 22 April 2016. Italian Republic v European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62006TJ0060%2801%29

98. Keating, V. C., & Schmitt, O. Ideology and influence in the debate over Russian election interference. International Politics, 1-15.

99. Kremlin Watch Report, 16 May 2017, Overview of countermeasures by the EU28 to the Kremlin's subversion operations. How do the EU28 perceive and react to the threat of hostile influence and disinformation operations by the Russian Federation and its proxies?

100. Krusteva, Desislava, Makshutova, Radoslava. Bulgaria: Legislative attempts to restrict disinformation in 2020, OneTrust DataGuidance, August 2020: https://www.dataguidance.com/opinion/bulgaria-legislative-attempts-restrict

101. Law No. 27/2021, Carta Portuguesa de Direitos Humanos na Era Digital, https://dre.pt/dre/detalhe/lei/27-2021-163442504,

102. Law on Misdemeanours against Public Order and Peace, https://www.zakon.hr/z/279/Zakon-o-prekr%C5%A1ajima-protiv-javnog-reda-i-mira,

103. Lex Generalis and Lex Specialis, https://www.spacelegalissues.com/lex-generalis-and-lex-specialis/

104. Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

105. Library of Congress, 'Germany: Network Enforcement Act Amended to Better Fight Online Hate Speech', https://www.loc.gov/item/global-legal-monitor/2021-07-06/germany-network-enforcement-act-amended-to-better-fight-online-hate-speech/

106. Lietuvos gynybos politikos Baltoji knyga, 2017, https://kam.lt/lt/gynybos_politika_490/aktualus_dokumentai_492/strateginiai_dokumentai_494.html

107. Lietuvos Respublikos karinė strategija, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2016 m. kovo 17 d. įsakymu V-252, https://kam.lt/lt/gynybos_politika_490/aktualus_dokumentai_492/strateginiai_dokumentai_494.html

108. Lietuvos Respublikos visuomenės informavimo įstatymas, https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr

109. Loi du 29 juillet 1881 sur la liberté de la presse, https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/,

110. LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/

111. Mark Young, *European Parliament approves EU Cybersecurity Act*, March 14th 2019, https://www.insideprivacy.com/international/european-union/european-parliament-approves-eu-cybersecurity-act/t .

112. Ministry of Foreign Affairs of Denmark, Strengthened safeguards against foreign influence on Danish elections and democracy, 7 September 2018, https://um.dk/en/news/newsdisplaypage/?newsid=1df5adbb-d1df-402b-b9ac-57fd4485ffa4

113. Nacionalinio saugumo strategija, 2021, https://www.e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/asr

114. O'Halloran, M., 'Government defeated on online advertising and social media Bill', 14 December 2017, https://www.irishtimes.com/news/politics/oireachtas/government-defeated-on-online-advertising-and-social-media-bill-1.3327979

115. Online Advertising and Social Media (Transparence) Bill 2017, https://web.archive.org/web/20180506190500/http://www.oireachtas.ie/documents/bills28/bills/2017/15017/b15017d.pdf,

116. Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional, https://boe.es/boe/dias/2020/11/05/pdfs/BOE-A-2020-13663.pdf

117. OSCE, Coronavirus response bill should not curb freedom of information in Romania, stresses OSCE Media Freedom Representative, https://www.osce.org/representative-on-freedom-of-media/449380

118. Overview of countermeasures by the EU28 to the Kremlin's subversion operations https://www.kremlinwatch.eu/userfiles/overview-of-countermeasures-by-the-eu28-to-the-kremlin-s-subversion-operations_15273205278094.pdf

119. Penal Code of Estonia https://www.legislationline.org/download/id/9098/file/EST_CC_as%20of%20May%202021.pdf

120. Pérez, Enrique, 'El Gobierno plantea cambios legales para frenar los bulos en internet: qué castigos contempla ya la ley y por qué su regulación genera tantas dudas', 7 April 2020, https://www.xataka.com/legislacion-y-derechos/gobierno-plantea-cambios-legales-para-frenar-bulos-internet-que-castigos-contempla-ley-que-su-regulacion-genera-tantas-dudas

121. Pilić, M., Pilić, M. (2021) Infodemija u doba covida-19: kaznenopravni i sigurnosni aspekt. Polic. sigur. 3, https://hrcak.srce.hr/file/385061

122. Polyák Gábor, Mertek, Hungary's Two Pandemics: COVID-19 and Attacks on Media Freedom, European Centre for Press and Media Freedom, 2020, https://www.ecpmf.eu/wp-content/uploads/2020/06/Legal-opinion-Hungary_2020.pdf

123. Presidency of the Council, "Outcome of the Justice and Home Affairs Council meeting of 8 and 9 December 2016, No. 15391/16.

124. Presidency of the Portuguese Republic, Article 6 of the Portuguese Charter on Human Rights in the Digital Age, Application send to the Constitutional Court, https://www.presidencia.pt/atualidade/toda-a-atualidade/2021/07/artigo-sexto-da-carta-portuguesa-dos-direitos-humanos-na-era-digital/

125. Proposals to Act amending the Criminal Code of Denmark (Illegal influence activities), https://www.ft.dk/ripdf/samling/20181/lovforslag/l95/20181_l95_som_fremsat.pdf

126. Questions and Answers - EU Cybersecurity, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_19_3369

127. Reference of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, OL ITA 1/2018, 20 March 2018, https://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL-ITA-1-2018.pdf,

128. Reporters without borders, New Greek law against disinformation endangers press freedom, https://rsf.org/en/news/new-greek-law-against-disinformation-endangers-press-freedom,

129. Ronan, Ó F., Helberger, N., Appelman, N. (2021). "The perils of legally defining disinformation". Internet Policy Review 10 (4), https://policyreview.info/articles/analysis/perils-legally-defining-disinformation

130. Scott, G. (2017) Defamation and Insult Laws in the OSCE Region: A Comparative Study, https://www.osce.org/files/f/documents/b/8/303181.pdf

131. Sigutė Stankevičiūtė, doctoral dissertation "Asmens duomenų rinkimo elektroninėje erdvėje teisėsaugos ir žvalgybos tikslais reglamentavimas", 2020, Vilnius.

132. Sofia V., 'Tackling fake news, the Italian way', Resource Center on Media Freedom in Europe, 29 May 2018, https://www.rcmediafreedom.eu/Tools/Legal-Resources/Tackling-fake-news-the-Italian-way,

133. Spring 2017 Global Attitudes Survey, Pew Research Centre.

134. Štitilis, D., Pakutinskas, P., & Malinauskaitė, I. (2017). EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. Security Journal, 30(4), 1151-1168.

135. Stolton, Samuel, 'Facebook urges Ireland to hold off on political ads rules until EU legislation', Euractiv, Mar 30, 2021, https://www.euractiv.com/section/digital/news/facebook-urges-ireland-to-hold-off-on-political-ads-rules-until-eu-legislation/

136. T. Klimas, J. Vaiciukaitez, *The Law of Recitals in European Community Legislation*, July 2008,

137. Tackling Disinformation and Online Hate Speech: Case studies of 27 EU Member States, so far', Democracy Reporting International, February 2021, p. 14, https://digitalmonitor.democracy-reporting.org/wp-content/uploads/2021/02/Tackling-Disinformation-and-Online-Hate-Speech-27-Case-Studies.pdf

138. Țară în service, Dezinformare și siguranță națională - cum amenință știrile false să destabilizeze România, https://romania.europalibera.org/a/31566084.html,

139. The anti-coronavirus act, https://magyarkozlony.hu/dokumentumok/9b48945c85f190378f67e253337be4299edf743f/megtekintes

140. The Criminal Code of Denmark, https://danskelove.dk/straffeloven

141. The GFCE-MERIDIAN Good Practice Guide on Critical Information Infrastructure Protection for governmental policy-makers, https://www.tno.nl/media/8578/gpg_criticalinformationinfrastructureprotection.pdf

142. The Law Library of Congress, Global Legal Research Directorate, Government Responses to Disinformation on Social Media Platforms: Comparative Summary, https://www.hsdl.org/?view&did=835597

143. The Law of Recitals In European Community Legislation, https://nsuworks.nova.edu/ilsajournal/vol15/iss1/6/

144. The ruling of the Constitutional Court of Lithuania of 19 September 2005 'On the procedure for the dissemination of information not to be divulged to the public', https://www.lrkt.lt/en/court-acts/search/170/ta1309/content

145. The rulings of the Constitutional Court of Lithuania of 13 December 2004, 29 December 2004, 29 September 2005.

146. The Swedish Criminal Code, https://www.government.se/49f391/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf

147. Tworek, H., Leerssen, P. An Analysis of Germany's NetzDG Law, 15 April 2019, https://www.ivir.nl/publicaties/download/NetzDG_Tworek_Leerssen_April_2019.pdf

148. Weber, A. M., The Council of Europe's Convention on Cybercrime, 18 Berkeley Tech. L.J. 425.

Chapter 10 Appendixes

10.1 Moot Problem

Periphery elections

1. The Republic of Periphery is a small state with a population of 3 000 000, whose eastern border is also the external border of the European Union. As a former state of the socialist bloc, It regained its independence 30 years ago and joined the EU 15 years ago. There is a vibrant political scene in the state, with elections taking place every 4 years. It is also a country with one of the world's best internet connections, where the population receives most of the information from online news portals and social networks.

2. In the 2016 parliamentary elections, the ruling EUForIa party lost 20% of the vote (300,000 votes) to the new PExit party, a nationalist, anti-EU right-wing extremist party that wants to leave the EU. The EUForIa, together with the Neutral Party, still has a majority (55% together) in parliament and forms a governing coalition.

3. Allegations of possible interference in the US presidential election and the 2016 UK Brexit referendum, as well as the 2017 French parliamentary elections, have raised serious concerns in the Fringe government about the sudden rise of the PExit party and possible interference in the upcoming elections in the Republic of Periphery.

4. Even after the European Parliament announced[272] that foreign interference in the electoral process poses a serious threat to European democratic societies and often benefits anti-EU, right-wing extremist and populist candidates, the Government of the Republic of Periphery has decided to ensure protection against possible interference in elections planned in April 2020.

5. In November 2019 the Parliament of Periphery passed the Law on Responsible Elections (LRE), the preamble of which states that “interference in elections poses a serious threat to the democratic order of the state”. Article 3 of LRE prescribed that, in order to protect the electoral process from cyber incidents and the misinformation of citizens, the respective human rights to freedom of expression and the dissemination of information may be restricted during and before elections. According to Article 4 of LRE during the elections any factually incorrect or inaccurate information shall be considered to be misinformation whereas the author and publisher of such information will have a duty to prove the accuracy of such information or to publicly rebuke it. At the same time, this article established that the authority responsible for supervising such information is an official of the Ministry of Culture and Information. Article 5 of the LRE states that, during the election, the State Security Department has the right to immediately restrict access to any website or social network and to impose a penalty against author and publisher who engage in activities of disinformation, provided that state officials receive a written report on disinformation and subject to failure of the website’s operator to remove such information.

6. In March 2020 due to the threat of Covid-19 the quarantine was announced in most of the Member States of the European Union. From 18 March 2020 the Republic of Periphery imposed quarantine, border closure and restrictions on the movement of people. According to Article 144 of the Constitution of Periphery “In case of there is a threat to the constitutional order or the public order in

[272] 2.10.2019. European Parliament resolution on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP))

the State, the Parliament may declare a state of emergency in all or part of the territory of the State". Some other EU Member States imposed such restrictions as early as on 11 March 2020. Like many other European Union countries, the health care authorities of the Republic of Periphery were not prepared for the sudden spread of an unknown epidemic (such as Covid 19), leading to a shortage of medical masks, lung ventilators and other medical kits and equipment designated to fight airborne virus. Notwithstanding the application of the Covid-19 measures, the elections to be held in May 2020 were not cancelled or postponed.

7. On 5 March 2020, national television of Periphery published the latest party ratings. According to polls commissioned by the news agency ALTA, the EUForIa party would win the election by just 1%. The EUForIa party is supported mostly by older voters, especially those over 60.

8. During the election campaign which started in March 2020, PExit created a @TruePexitFacts channel on one of the most popular social networks, FaceChat.This channel was very popular among people and had 350,000 unique visitors. The social network has made attractive statements about perceived shortcomings in the EU, including the introduction of genetically modified products in EU-made goods, high EU membership costs, the imperialist nature of the EU and upon the announcement of quarantine – the complete inability of the EU to deal with the Covid-19 threat. Separately on 17 April 2020, two days before the elections, articles were published in this channel about the donation of eastern neighbouring country (non-EU Member State) of Periphery consisting of 5,000 medical masks and 5 lung ventilators, indicating "EU's solidarity is an illusion, because the EU has made no contribution to facilitate the survival of the people of Periphery , whereas our neighbours, who deal perfectly with Covid-19, support us with vital kits and equipment". The Ministry of Foreign Affairs of the Periphery informed on its website that the European Union sends 10,000 medical masks weekly to Periphery, and in total had sent 50 lung ventilators, but such information has not been published in order not to increase tension in society and to avoid inappropriate interpretations. At the same time, the Ministry of Foreign Affairs of the Periphery contacted an official of the Ministry of Culture for the evaluation of such statements.

9. The day before the election, on 18 April 2020, among other news stories a comment was made on the @TruePexitFacts channel about the lethal effects of Covid-19 on people at risk, which includes people over 55 years of age. The Commentator called for people to stay at home, as large gatherings and especially visits at the same premises pose a serious threat of contraction of a deadly disease. There has also been a regret that the current government does not care about peoples' health and has not postponed the elections or allowed people to vote electronically, which could have allowed for all the residents to cast a vote

10. On the same day an official from the Ministry of Culture received a complaint concerning the statement of 17 April 2020 provided on@TruePexitFacts channel and requested the PExit party to provide evidence to support such claims. PExit replied that such a request violated the freedom of expression and opinion of commentators guaranteed by the European Convention on Human Rights and did not provide information. Following such a response, the official of the Ministry of Culture and Information informed the Departmentof State Security about the desinformation performed by PExit, stating that the PExit party had not provided evidence on the accuracy of the claims.

11. Considering all this, the official of the Ministry of Culture, in accordance with Article 4 of the LRE, requested FaceChat to remove content from the @TruePexitFacts channel. FaceChat replied that the company does not control free speech issues and cannot remove content without a court ruling. An official of the Ministry of Culture and Information informed the Department of State Security of such a response.

12. On the evening of 18 April 2020 Electoral Commission contacted the State Security Department informing that it had received a comment encouraging them to refrain from voting. The State Security Department immediately closed access to the FaceChat website, i.e. restricted access to the FaceChat website on computers in the Republic of Periphery. The Department informed FaceChat that the website's availability was restricted on the grounds that FaceChat did not remove the propaganda contents from its website, as was reported by the official of the Ministry of Culture, and the Department of State Security in the context of state of emergency took the necessary steps to ensure democratic order. FaceChat and the Pexit political party, have exhausted its internal legal remedies, appeals to the ECtHR requesting to determine that:

1. Periphery cannot rely on Article 15 of the ECHR to justify the imposed restrictions on human rights;
2. The obligation imposed by Periphery to prove the accuracy of opinion infringes Article 10 of the ECHR;
3. The closure of the FaceChat website in Republic of Periphery performed by Peripherian officials violates Article 10 of the Convention;
4. Periphery has violated the positive obligation to guarantee the right to free elections enshrined in Article 3 of Protocol 1 to the Convention.

The State of the Periphery states in its position that:

1. Periphery may invoke Article 15 of the ECHR to justify the imposed restrictions on human rights;
2. The obligation imposed by Periphery to prove the accuracy of opinion is without prejudice to Article 10 ECHR.
3. The closure of the FaceChat website in Republic of Periphery performed by Peripherian officials does not infringe Article 10 of the ECHR;
4. Periphery neither by its actions nor omissions violated the right to free elections enshrined in Article 3 of Protocol 1 to the Convention.

10.2 Template for the collection of legal challenges

Title: <SHORT TITLE>		
Reporter: <NAME>	**Organization:** <ORGA>	**Email:** <EMAIL>
Related Work Package (if applicable): -		
Short Description: <TEXT>		
Desired Solution: <TEXT>		
Current Workaround (if applicable): <TEXT>		
Further Resources (links, examples, etc): [1] <TEXT>		
Comments: This is a dummy report containing some text		

10.3 Provisions establishing responsibility for disinformation

Table 2: Provisions establishing responsibility for disinformation

Country	Prohibited conduct		Mental element	Harm	Punishment	Legal basis
Italy		false, exaggerated, or biased news	maliciously	which may undermine public order	- arrest for up to 3 months, or - a fine of up to 309 Eur	Article 656, Criminal Code
Malta	spreads	false news	maliciously	which is likely to alarm public opinion or disturb public good order or public peace or to create a commotion among the public or among certain classes of the public.		Article 82 of the Criminal Code
Romania	communicates or disseminates	false news, data or information or of falsified documents	knowing their false character	which endangers the national security	imprisonment from 1 to 5 years	Article 404, Criminal Code
Greece	publicly or via the Internet spreads or disseminates in any way	false news	maliciously	causing concern or fear to the public or undermining public confidence in the national economy, the country's defense capacity, or public health	By imprisonment of at least 3 months, or a fine - if repeated, of at least 6 months) to 5 years, and a fine	Article 191(1), Penal Code
	publicly or via the Internet spreads or disseminates in any way	false news	by negligence	causing concern or fear to the public or undermining public confidence in the national economy, the country's defense capacity, or public health,	by imprisonment of up to 1 year or a fine	Article 191(2), Penal Code
Slovakia	spreads	an alarming message which is untrue or by committing any other similar act	intentionally	a serious danger to at least part of the population in some area	by imprisonment for up to 2 years	Article 361 (1), Penal Code
	reports	a false alarming news, or other similar act referred to in paragraph 1, to a legal entity or the Police Force or other State authority or *to the mass media*	maliciously	may cause serious concerns among the population of a certain location or at least a part	by imprisonment of 1 to 5 years. By imprisonment of 3 to 8 years, if seriously impairs economic operation or economic activities of a legal entity or the activity of a State authority or other particularly serious consequence	Article 361 (2), Penal Code

Country	Prohibited conduct		Mental element	Harm	Punishment	Legal basis
					through its commission.	
Hungary	claims or spreads	any falsehood or any distorted fact with regard to the public danger	maliciously	that is capable of causing disturbance or unrest in a larger group of persons at the site of public danger	by imprisonment for up to 2 years	Article 337 (1), Criminal Code
	claims or spreads	a falsehood or a distorted fact before a large public during an emergency legal regime	maliciously	in a way that is suitable for obstructing or preventing successful defence	by imprisonment for up to 5 years	Article 337 (2), Criminal Code
	states or disseminates	any untrue fact or giving the impression that there is imminent danger for the occurrence of an event	maliciously	that is likely to harm the general public and cause harm to the public	by imprisonment from 1 to 5 years, if the threat of public endangerment has resulted in a grave disturbance of public peace	Article 338, Criminal Code
Spain	affirm or simulate	false situation of danger to the community or producing damages	knowingly	leading to the provision of assistance to another and provoking the mobilization of the police, assistance and rescue services	by imprisonment from 3 months and 1 day to 1 year	Article 561, Penal Code
Austria	publicly disseminates	false information about circumstances that may prevent voters from voting or exercising their right to vote at that time,	maliciously	when the retaliation campaign is ineffective in terms of time	by imprisonment for up to 6 months or a fine of up to 360 days	Article 264 of the Criminal Code
Bulgaria	transmits	over the radio, by telephone, or in some other way false calls or misleading signals for help, accident, or alarm	maliciously	-	by imprisonment up to 2 years	Article 326 (1) of the Criminal Code*
	transmits	over the radio, by telephone, or in some other way false calls or misleading signals for help, accident, or alarm	maliciously	resulting in considerable harmful consequences, the punishment shall be	by imprisonment ri t to 5 years and a fine of BGN 500 to 2000.	Article 326 (2) of the Criminal Code*
Croatia	invents or spreads	false news	maliciously	that will disturb the peace and tranquility of citizens	by fine or by imprisonment for up to 30 days	Article 16 of the Law on Misdemeanours against

Country	Prohibited conduct		Mental element	Harm	Punishment	Legal basis
						Public Order and Peace
Cyprus	publicises	any form of false news or news	maliciously	that can potentially harm civil order or the public's trust in the State's authorities or cause fear or worry among the public or harm civil peace and order in any way	by imprisonment of up to 2 years or with a fine that cannot exceed 1500 pounds or both of those sentences	Article 50 of the Criminal Code
Czech Republic	spreads	alarming news that is untrue	maliciously	causes a threat of serious concern to at least a portion of the population of a certain area	by imprisonment or up to 2 years or by prohibition of activity.	Section 357 (1), Penal Code*
	communicates	the news referred to in Subsection 1 or other untrue news	maliciously	capable of causing precautions leading to a risk of serious concern of at least a portion of population of a certain place or an unfounded rescue operation of the integrated emergency system to court or to a police authority of the Czech Republic, to a state administration authority, local self-administration authority or another public authority, to a legal person, natural person who is an entrepreneur or a mass communication media,	by imprisonment for 6 months to 3 years or by prohibition of activity.	Section 357 (2), Penal Code*
Denmark	spreads	false or misleading information	maliciously	which can affect the price of securities or similar assets significantly	by a fine or by imprisonment of up to 1 year and 6 months.	Section 296 (1) of the Penal Code
			gross negligence	which can affect the price of securities or similar assets significantly	by a fine or, in aggravating circumstances, imprisonment for any term not exceeding 4 months	Section 296 (2) of the Penal Code
	spreads	false or misleading information	intentional	which can affect the price of goods, real estate or similar assets significantly		Section 297 (1) of the Penal Code
			gross negligence	which can affect the price of goods, real estate, or similar assets significantly,	by a fine or, in aggravating circumstances, imprisonment for any term not exceeding 4 months	Section 297 (2) of the Penal Code

Country	Prohibited conduct		Mental element	Harm	Punishment	Legal basis
	does	something whereby foreign intelligence services are enabled or assisted to act immediately or directly within the territory of the Danish state, including cooperation to carry out advocacy activities	maliciously	with a view to influence decision-making or public opinion formation,	by imprisonment for up to 6 years.	Section 108 (1) of the Penal Code
		the same act in the case of intelligence relating to military matters, or the enterprise takes place during war or occupation, and in connection with the elections and voting that are covered by section 116	maliciously		by up to 12 years of imprisonment	Section 108 (2) of the Penal Code
France	have surprised or diverted votes, determined one or more voters to abstain from voting,	with the help of false news, slanderous rumors, or other fraudulent maneuvers	maliciously		By imprisonment for one year and a fine of 15,000 euros.	Article L97 of Electoral Code

**The provisions prohibit 'false alarm'.*