DOI: https://doi.org/10.24833/0869-0049-2024-1-107-122

Исследовательская статья
УДК: 341.3
Поступила в редакцию: 03.07.2023
Принята к публикации: 16.02.2024

Елизавета Борисовна КИРИЛЛОВА
Посольство Российской Федерации в Королевстве Швеция
Гьёрвеллсгатан 31, 112 60 Стокгольм, Швеция
ebkirillova@mid.ru
ORCID: 0009-0004-4022-5279

СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА ОБ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ В РОССИИ И ШВЕЦИИ

ВВЕДЕНИЕ. *В статье представлен комплексный анализ нормативно-правовой базы, регулирующей область информационных технологий (далее – ИТ) в России и Швеции, проведена сравнительная оценка ключевых правовых инструментов, концепций и подходов к регулированию, включая ответственность за киберпреступления, процедуры лицензирования, практику стандартизации и безопасность критической информационной инфраструктуры. Кроме того, в статье рассматриваются роли и функции основных регулирующих органов в обеих странах.*

МАТЕРИАЛЫ И МЕТОДЫ. *Статья подготовлена на основе соответствующих правовых актов России и Швеции. Несмотря на наличие отдельных законов, полностью посвященных ИТ, некоторые положения можно найти в других видах правовых документов (например, в уголовных кодексах или постановлениях правительства). С помощью сравнительного подхода в исследовании очерчиваются рамки и полномочия государственных институтов, осуществляющих регулирование в сфере ИТ.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *И в России, и в Швеции наблюдается сходство в определении основных понятий, таких как критическая инфраструктура, что отражает общую проблематику, связанную, например, с вопросами безопасности. Основные законы в области ИТ содержат спектр ключевых терминов, включая, но не ограничиваясь, информационно-коммуникационной сетью / электронной сетью коммуникаций, оператором информационной системы, а также защитой информации / безопасностью сети и информационной системы. Хотя список ключевых определений может показаться довольно сходным, шведское законодательство, как правило, предлагает более широкие определения с целью охвата более общих областей в рамках ИТ, в то время как российские законодатели фокусируются на применении более конкретных терминов. Однако если в Швеции законодательство тесно связано с нормативной базой Европейского союза (далее – ЕС), то в России применяется более широкий подход, учитывающий новые технологические вызовы, такие как искусственный интеллект. В заключение следует отметить, что для эффективного регулирования ИТ необходимо найти баланс между согласованностью на международном уровне и возможностью адаптации на национальном, что позволит обеспечить высокий уровень кибербезопасности, стимулировать инновации и сохранить гибкость регулирования в динамичной цифровой среде.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Швеция делает ставку на внедрение нормативных актов ЕС, что имеет свои преимущества, такие как гармонизация, внедрение признанной*

на международном уровне практики, облегчение доступа на рынок и т. д. Однако такой подход может ограничить возможности страны по удовлетворению своих специфических потребностей и повлечь за собой дополнительное бремя, связанное с соблюдением директив ЕС. Более того, изменения в нормативных актах ЕС могут привести к необходимости обновления внутреннего законодательства, что потенциально может вызвать возникновение законодательных пробелов или коллизий, особенно в такой сфере, как ИТ. Сегодня, когда на повестке стоят искусственный интеллект и его риски, невозможно оставаться в стороне и ждать, пока международное сообщество договорится о применимом регулировании.

КЛЮЧЕВЫЕ СЛОВА: *IT-право, кибербезопасность, электронные коммуникации, критическая инфраструктура, законодательство Швеции, киберпреступления, безопасность сетей и информационных систем, регулирование информационных технологий, российское законодательство об информационной безопасности*

ДЛЯ ЦИТИРОВАНИЯ: Кириллова Е.Б. 2024. Сравнительно-правовой анализ законодательства об информационных технологиях в России и Швеции. – *Московский журнал международного права.* № 1. С. 107–122. DOI: https://doi.org/10.24833/0869-0049-2024-1-107-122

Автор заявляет об отсутствии конфликта интересов.

INTERNATIONAL AND NATIONAL LAW

DOI: https://doi.org/10.24833/0869-0049-2024-1-107-122

Research article
UDC: 341.3
Received 3 July 2023
Approved 16 February 2024

Elizaveta B. KIRILLOVA
Embassy of the Russian Federation in the Kingdom of Sweden
Gjörwellsgatan 31, 112 60 Stockholm, Sweden
ebkirillova@mid.ru
ORCID: 0009-0004-4022-5279

COMPARATIVE LEGAL ANALYSIS OF IT LEGISLATION IN RUSSIA AND SWEDEN

INTRODUCTION. *This article provides a comprehensive analysis of the regulatory frameworks governing the information technology (IT) sector in both Russia and Sweden and encompasses a comparative assessment of key legal instruments, concepts, and regulatory approaches, including the responsibility for cybercrimes, licensing procedures, standardization practices, and the safety of critical informational infrastructure. Additionally, this article examines the roles and functions of major governing authorities in both countries.*

MATERIALS AND METHODS. *The article is based on relevant legal acts of Russia and Sweden. While there are certain specific laws focused entirely on the informational technologies, some provisions can be found in other types of legal documents (for example criminal codes or governmental regulations). Employing a comparative approach, the study delineates the scope and authority of state institutions involved in the IT sphere.*

RESEARCH RESULTS. *Both Russian and Sweden exhibit similarities when it comes to definition of essential concepts such as critical infrastructure, reflect shared concerns regarding for example security issues. Main laws in the area of information technology contain a spectrum of key terms, including but not limited*

to information and communication network / electronic communication network, information system operator, and information protection / network and information system security. Although the list of key definitions may appear quite similar, the Swedish legislation tends to offer broader definitions with the intention of encompassing larger domains within IT technologies, while the Russian legislators focus on more specific terms. However, while Sweden aligns closely with European Union (EU) regulatory framework, Russia adopts a more expansive approach, addressing emerging technological challenges such as AI. In conclusion, achieving effective IT regulation necessitates finding a balance between international consistency and national adaptability to ensure strong cybersecurity, foster innovation, and maintain regulatory flexibility in a dynamic digital environment.

DISCUSSION AND CONCLUSIONS. *Sweden's reliance on implementing EU regulations has its benefits such as harmonisation, interoperability, adopting the internationally recognised practices, easier market access, etc. However, this approach may limit the country's ability to meet its specific needs and may mean additional administrative burdens associated with compliance with EU directives. Moreover, changes in EU regulations could lead to a necessity to update domestic laws, potentially causing regulatory vacuum or legal collisions, especially in such sphere as the IT sector. Nowadays, when for example the AI and its risks are on the daily agenda one can not look away and wait for the international community to agree on the applicable regulation.*

KEYWORDS: *IT law, cybersecurity, electronic communications, critical infrastructure, Swedish legislation, cybercrimes, Network and Information System Security, regulation of informational technologies, Russian laws on information security*

FOR CITATION: Kirillova E.B. A Comparative Legal Analysis of IT Legislation of Russia and Sweden. – *Moscow Journal of International Law.* 2024. No. 1. P. 107–122. DOI: https://doi.org/10.24833/0869-0049-2024-1-107-122

The author declares the absence of conflict of interest.

1. Introduction

The analysis of the regulation of the informational technologies should begin with a definition of cyberspace as an object of the international law. "Is cyberspace an object of international law if there is no universal international treaty on it? <…> In international legal scholarship considers alternative scenarios for the transition to 'transnational governance' cyberspace, instead of its current mostly national and corporate governance by US-registered IT giants" [Vylegzhanin, Shtodina 2022:227-239].

The issue of cyberspace, or, more particularly, social media, being governed by a few IT-giants, is also addressed by D. Westman from the Swedish Law and Informatics Research Institute: "However, the fact that these new important arenas for the exercise of freedom of expression are controlled by a few dominant commercial actors operating in an international market poses legal challenges" [Westman 2020:676].

Cyberspace itself is a complex and dynamic environment that encompasses the digital realm where computer systems, networks, and data interact. In the context of international law, defining cyberspace has been a challenge due to its intangible and borderless nature.

In the Doctrine of Information Security of the Russian Federation, the *information sphere* is understood as "the totality of information, informatization objects, information systems, sites in the information and telecommunication network 'Internet' (hereinafter – the 'Internet'), communication networks, information technologies, subjects whose activities are related to the formation and processing of information, development and use of these technologies, ensuring information security, as well as the totality of mechanisms for regulating the relevant social relations, and also the totality of mechanisms for regulating the information security of the Russian Federation"[1].

Russia "was a pioneer of international cooperation in ensuring ICTs security and consistently de-

[1] Decree of the President of the Russian Federation № 646 "On Approval of the Doctrine of Information Security of the Russian Federation". URL: http://www.kremlin.ru/acts/bank/41460 (accessed date: 08.10.2023).

fends the position that the only way to counter threats in the information sphere is within the framework of international cooperation in ICTs security" [International… 2021:10].

However, as the authors of an IMEMO monograph "International Security, Strategic Stability and Information Technologies" rightly point out, "One of the main problems remains the lack of a unified international legal regime governing the ICT space, as today only some generally accepted norms of international law and various national legislations apply" [Romashkina, Markov, Stefanovich 2020:21].

On May 15, 2023, Russia together with Belarus, North Korea, Nicaragua and Syria as co-sponsors, submitted the Concept of the UN Convention on Ensuring International Information Security as an official document of the 7^{7th} session of the UN General Assembly. "A growing need for the peaceful use of information and communications technologies, as well as for their use for the common good of humankind and further social and economic development of all States"[2] was emphasised.

During the 78th session Russia submitted a draft resolution *"Developments in the Field of Information and Telecommunications in the Context of International Security"*. Sweden, eagerly following into the EU and the US steps, voted against it. The explanation given by the EU on behalf of all member states (and so-called "candidate countries") was rather vague: "The EU considers that the resolution could have better represented the fragile consensus achieved in the Open Ended Working Group, its preceding processes and previous consensus resolutions. Principally, the draft resolution fails to reference the cumulative and evolving framework for responsible State behaviour in the use of ICTs"[3].

In Sweden there is a definition of a *"cyber domain"*, given by the Armed Forces in the Military strategic doctrine: "the cyber domain consists of digital information systems and electronic communication services, and the data stored in, processed by, or transmitted through them"[4].

The report of Swedish Total Defence Research Institute "Operations in the cyber domain – an inventory of Swedish research emphasise that Swedish definition" emphasises that the Swedish definition "reflects the fact that the cyber domain:

1) is global and borderless;
2) uses electronics, the electromagnetic spectrum and IT;
3) is used for the creation, storage, modification, exchange or exploitation of information;
4) allows for remote action because of infrastructures that are interconnected and interdependent;
5) encompasses both attack and protection, as well as intelligence, propaganda and creation of certain opinion" [Karzlen, Granlund, Wedlin 2018:9].

"With comparatively large public administrative sectors, the Scandinavian countries, especially Sweden, had early on started to invest substantially in computers for the public sector. Consequently, there also existed an interest in finding ways of employing the new technology in the legal domain and in 1966 it was decided that a standing committee for the development of IT for the judiciary should be established. Members included the heads of the authorities in the legal sector and a representative from the parliament. The work was led by the state secretary at the Ministry of Justice" [Wahlgren 2023:232]. In Sweden "legal informatics" (swed. "rättsinformatik" is recognised as a research field.

The forthcoming article delves into the legislative approaches of both Russia and Sweden in defining such technologies. The analysis focuses on key legal documents, examining the terminology employed within these acts and its contextual significance.

A special attention, in my opinion, ought to be directed towards the dimensions of information security and the safeguarding of critical information infrastructure. Unquestionably, the regulatory role played by public authorities, encompassing control and oversight functions, as well as the licensing procedures and pertinent standards applicable to this domain should be included.

---

[2] The Concept of the UN Convention on Ensuring International Information Security. URL: http://www.scrf.gov.ru/media/files/file/cSYQQBkOHCz1AaOfPwZJFsVfP3EXQjEi.pdf (accessed date: 09.10.2023).

[3] EU Explanation of Vote: UN General Assembly 1st Committee: Information and telecommunications in the context of international security. URL: https://www.eeas.europa.eu/delegations/un-new-york/eu-explanation-vote-un-general-assembly-1st-committee-information-and-telecommunications-context_en?s=63 (accessed date: 10.11.2023).

[4] Militärstrategisk doktrin (MSD 22), Sveriges Försvarsmakt. P. 55. URL: https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/doktriner/msd-22.pdf (in Swedish) (accessed date: 10.10.2023).

2. Main laws regulating IT-sphere

We'll start with examining the objectives of legal regulation concerning informational technologies in both Russia and Sweden, along with the pivotal terminology utilized. For this purpose, let us compare Russian *Federal Law № 149-FZ on Information, Informational Technology and the Protection of Information* and the Swedish *Electronic Communications Act*.

Russian Federal Law "regulates relations arising in:

1) exercising the right to search, receipt, transfer, production and dissemination of information;
2) applying informational technologies;
3) ensuring protection of information"[5].

The Electronic Communications Act aims to provide individuals and authorities with "access to secure and efficient electronic communications and to the broadest choice of such services, their price, quality and capacity"[6]. The Act applies to "electronic communications networks and electronic communications services and related facilities and services, as well as other types of radio use"[7].

The Act on information security for essential and digital services (Lag om informationssäkerhet för samhällsviktiga och digitala tjänster) imposes requirements on certain providers of essential and digital services. A central part of the law is therefore "to define who is to be considered such a provider and what constitutes an essential or digital service. It also describes the suppliers' obligation to work in a risk-based manner and carry out preventive work to prevent incidents. Once an incident has occurred, there are strict requirements regarding reporting and management" [Wendleby 2022:5].

2.1. The comparison of the key terms of the Federal Law on Information and the Electronic Communications Act

The following terms exist in both legal acts and, while slightly differ, essentially represent the same concept.

Russia: *Information and Telecommunication Network* means "a technological system intended to transmit via communication lines the information further accessed using computation devices"[8].

Sweden: E*lectronic communications network* means "a transmission system and, where applicable, switching or routing equipment and passive network elements and other resources which permit the conveyance of signals, by wire or by radio waves, by optical means or by other electromagnetic transmission media, irrespective of the type of information transmitted"[9].

As we already can see, *Electronic Communications Network* encompasses a broader scope. Because of a definition as a transmission system, it includes switching or routing equipment, passive network elements, and other resources. The primary purpose is to convey signals through various transmission media, regardless of the type of information being transmitted, while the *Information and Telecommunication Network* is meant to be a network designed to transmit information through communication lines, with subsequent access facilitated by computational devices.

Russia: *Information System Operator* means an individual or a legal entity operating an Information System, including processing the data contained in its databases[10].

Sweden: *operator* "means the provider or intended provider of a public electronic communications network or an associated facility"[11].

Here the Russian definition of an *Information System Operator* refers to an individual or legal entity engaged in operating an Information System. The scope includes the processing of data within its databases, indicating a focus on managing information systems and the associated data. The swedish definition of an *operator* again implies a broader perspective, incorporating entities involved in offering or intending to offer public electronic communication networks or related facilities.

---

[5] Federal Law № 149-FZ on Information, Informational Technology and the Protection of Information (hereinafter referred as "Federal Law on Information"). Art. 1. URL: https://eais.rkn.gov.ru/docs.eng/149.pdf (accessed date: 12.04.2023).

[6] The Electronic Communications Act 2022:482 (Lag 2022:482 om elektronisk kommunikation) (hereinafter referred as "the ECA"). Kap. 1 § 1. URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482 (In Swedish) (accessed date: 12.04.2023).

[7] The ECA. Kap. 1 § 2.

[8] Federal Law on Information. Art. 2.

[9] The ECA. Kap. 1 § 7.

[10] Federal Law on Information. Art. 2.

[11] The ECA. Kap. 1 § 7.

Russia: *Protection of information* "shall represent the undertaking of legal, organizational and technical measures towards:

1) ensuring protection of information against any illegal access, destruction, modification, blocking, copying, supply, dissemination and also against other illegal actions in respect of that information;

2) observance of confidentiality of information of limited access;

3) realization of the right of access to information"[12].

Sweden: *the security of network and information system* means "the ability of electronic communications networks and services to withstand, at a given level of confidence, events that undermine the availability, authenticity, accuracy or confidentiality of the networks or services, of the data stored, transmitted or processed, or of the related services offered by or accessible through those electronic communications networks or services"[13].

According to C. Trenta (Ph.D, Associate Professor of Tax Law at Örebro University), cybersecurity is more than its technological or economical and sometimes political applications. "While traditionally classified as a field within computer science, cyber-security has been cast more recently as an interdisciplinary area straddling policymaking, computer science, management, and the social sciences" [Trenta 2021:101].

"The area of law dealing with cybersecurity a field-spanning construct requiring coordinated interpretation and the application of a rather large and diverse array of legal sources". This legislative area could be defines as the "collaborative cybersecurity law" framework. ENISA (The European Union Agency for Cybersecurity) "also treats cybersecurity as an umbrella concept including information security, network and information systems security" [Trenta 2021:106].

Comparing the Russian and Swedish approach, we can see that Russian definition of *Protection of information* means a multifaceted approach involving legal, organizational, and technical measures for information protection and aims at comprehensive protection against unauthorized actions against information. While Swedish term *the security of network and information system* emphasizes the ability of networks and services to withstand events, indicating a focus on the overall security and robustness of electronic communications infrastructure and aims at maintaining the resilience of electronic communications networks and services, considering the confidence level and potential events that may undermine various aspects.

The Act on information security for essential and digital services 2018:1174 (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) complements the definition of the electronic communication network. According to this Act:

Electronic communications network is an "electronic communications network in accordance with Chapter 1. Section 7 of the Electronic Communications Act (2022:482) and

1) a device or a group of devices that are interconnected or related to each other, one or more of which carry out automatic processing of digital data through a programme; or

2) digital data that is stored, processed, retrieved or transmitted for the purpose of its operation, use, protection and maintenance"[14].

The same law provides, for example, a Swedish understanding go the search engine. So, *internet search engine* means "a service that allows users to search virtually any website or website in a particular language by requesting any topic in the form of a keyword, phrase or other input, and returns links containing information about the requested content"[15].

The Russian federal law states: "*a search engine* is an information system that searches the Internet at the user's request for information of a certain content and provides the user with information on the page index of an Internet site to access the requested information located on Internet sites belonging to other persons, except for information systems used to perform state and municipal functions, provide state and municipal services, as well as to perform other public powers, provided by federal laws"[16].

---

[12] Federal Law on Information. Art. 16 p.1.

[13] The ECA. Kap. 1 § 7.

[14] The Act on information security for essential and digital services 2018:1174 (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) (hereinafter referred as "Lag 2018:1174"). § 2. URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174 (In Swedish) (accessed date: 20.04.2023).

[15] Lag 2018:1174. § 2.

[16] Federal Law on Information. Art. 2.

Here, *Internet Search Engine* encompasses a broad range of services that facilitate searching across the internet, allowing users to access information from various sources based on their queries. While the Swedish definition of a *search engine* excludes information systems used for state and municipal functions, provision of state and municipal services, and other public powers from possible search results.

3. Critical informational infrastructure and its legal protection in Russia and Sweden

Firstly, it is essential to comprehend the meaning of the term "critical informational infrastructure" through a thorough examination of the relevant laws and regulations.

In Russia the key legal act is Federal Law № 187-FZ "About safety of critical information infrastructure of the Russian Federation".

"*Critical information infrastructure* – objects of critical information infrastructure, and also electronic communication networks used for the organization of interaction of such objects.

Objects of critical information infrastructure – information systems, information and telecommunication networks, automated control systems of subjects of critical information infrastructure.

Subjects of critical information infrastructure – state bodies, public institutions, the Russian legal persons and (or) individual entrepreneurs to whom on the property right, leases or on other legal cause belong *the information systems, information and telecommunication networks, automated control systems functioning in the field* of health care, science, transport, communication, energy, the bank sphere and other spheres of the financial market, fuel and energy complex in the field of atomic energy, the defense, space-rocket, mining, metallurgical and chemical industry, the Russian legal entities and (or) individual entrepreneurs who provide interaction of the specified systems or networks"[17].

Russia criminalizes three "unlawful forms of interference with critical information infrastructure objects: unlawful access; creation and distribution of malicious software; violation of the rules of operation of means of storing, processing or transmitting computer information; violation of the rules of operation of means of storing, processing or transmitting computer information" [Efremova 2022:88].

Swedish *Act on information security for essential and digital services 2018:1174* (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) provides a complete list of sectors of the economy which are considered essential: energy, transport, banking, financial market infrastructures, medical and health care, drinking water transport and distribution, digital infrastructure and digital services. Online marketplaces, online search engines, cloud computing services are all considered digital services. …point that this act "does not cover the sectors of production and distribution of district heating/cooling, chemical process industry, or electronic communications" [Appelgren, Zouave 2021:17].

In Sweden the provider of essential and digital services are obliged to rapport IT-incident to the Civil Contingencies Agency. "National strategy for preventing the emergence of terrorism, prevent terrorist attacks and prepare for the eventuality of a terrorist attack (2011/12:73), includes important measures such as strengthening IT security. The document refers to the work in order to prevent major cyber-attacks aimed at socially important IT systems" [Wennerström 2015: 48].

We can conclude that, despite some differences in wording, both in our country and in Sweden, the concept of critical infrastructure generally includes similar sectors. Both terms refer to the vital services provided in key sectors such as energy, transportation, banking, finance, healthcare, water supply, digital infrastructure, and digital services.

4. Liability and responsibility for breaches of the law and IT-related crimes

Both Russia and Sweden impose a duty on subjects of critical information infrastructure actors to immediately report all computer incidents to the competent governmental authority.

In the Swedish law, penalties for breaches of its requirements are specified directly in the text of § 29-36. Such a measure is a fine of 5 000 to 10 million SEK[18] imposed by the supervisory authority for

[17] Federal Law № 187-FZ About safety of critical information infrastructure of the Russian Federation (hereinafter referred as "FZ-187"). Art. 2. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (in Russ.) (accessed date: 30.04.2023).

[18] Lag 2018:1174. § 30.

failure to register as a critical service provider in good time with the supervisory authority or to report incidents, as well as for failure to take appropriate security measures[19].

The Russian Federal Law specifies liability for failure to comply with its requirements[20] (Article 14), but a specific list is contained in Article 13.12.1 of The Code of Administrative Offences. Fines for officials can vary from 10 to 50 thousand rubles, for legal entities – from 50 to 500 thousand roubles.

Swedish law makes no distinction for individuals or legal entities and the amount of the fine should be determined according to the damage caused.

While violations of legal requirements concerning critical information infrastructure are subject to administrative liability in Russia and fines in Sweden, a broader range of offences categorized as "computer crime" incur criminal responsibility in both states.

Criminal Code of the Russian Federation lists crimes in the sphere of commuter information in Chapter 28: illegal accessing of computer information; creation, use and dissemination of harmful computer programs; violation of rules for the operation of computer data storage, processing or transmission facilities and telecommunications networks; unlawful interference with the critical information infrastructure of the Russian Federation; violation of the rules of centralized administration of technical means of counteracting threats to the stability, security and integrity of the functioning of the information and telecommunications network "Internet" and the public communications network on the territory of the Russian Federation.

The Swedish Criminal Code essentially reduces the entire range of punishable computer crimes to illegal access to data and focuses specifically on breaches of data security with relatively limited penalties. It is safe to say that the broader scope, provided in the Code of the Russian Federation suggests a more comprehensive approach to addressing cybersecurity threats and protecting critical information infrastructure.

"A person who unlawfully obtains access to information intended for automatic processing, or unlawfully alters, erases, blocks or, in a register, inserts such information, is guilty of breach of data security and is sentenced to a fine or imprisonment for at most two years. The same applies to a person who seriously disturbs or impedes the use of such information in an unlawful way through some other similar measure.

Act 2014:302. If the offence is gross, the person is guilty of gross breach of data security and is sentenced to imprisonment for at least six months and at most six years. When assessing whether the offence is gross, particular consideration is given to whether the act caused serious damage, or related to a large quantity of information, or was otherwise of a particularly dangerous nature"[21].

However, Ulrik Franke, senior researcher, RISE Research Institutes of Sweden states that lawmakers work should be done from the perspective of the possible economical consequences of the cybercrimes. The cybersecurity center should provide experts conduct the analysis – similar process has already be done for example in the area of climate policy – when The National Institute of Economic Research (Konjunkturinstitutet) prepared the environmental economic research [Franke 2020:65].

U. Maunsbach and P. Lindskoug explore the possibilities of international private law to be applied to the cases of cross-border intellectual rights infringement which took place in the cyberspace. For Sweden, the answers to questions regarding jurisdiction, according to them, "must furthermore be divided into two parts since the answers depend on whether or not the defendant is domiciled in a Brussels or Lugano state (e. g. a country where the Lugano Convention (Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) or the Brussels I Regulation (Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters) are applicable) or in a country outside of this area" [Maunsbach, Limdskoug 2010:310]. However, this rule applies mostly to EU and EEA states.

But in case "the defendant is domiciled outside the Brussels/Lugano-area there is no directly applicable law in support of jurisdiction in cross-border infringement cases" [Maunsbach, Limdskoug

[19] Lag 2018:1174. § 29.

[20] FZ-187. Art. 14.

[21] The Swedish Criminal Code (Brottsbalken, SFS 1962:700) (hereinafter referred as "Brottsbalken"). Sec. 9c. URL: https://www.government.se/4a4563/contentassets/7a2dcae0787e465e9a2431554b5eab03/the-swedish-criminal-code.pdf (In Swedish) (accessed date: 02.05.2023).

2010:310]. Instead it is suggested to carefully apply the Swedish Code of Judicial Procedure (Den svenska rättegångsbalken) by analogy. By doing so, suggest the authors, "a Swedish Court can be competent to try disputes concerning cross-border transactions" [Maunsbach, Limdskoug 2010:311]. General rules of jurisdiction, used in the international private law, should be applied as well.

The rule, most likely to be applied by the Swedish court to the infringement of registered intellectual property rights, suggest U. Maunsbach and P. Lindskoug, would be the exclusive jurisdiction of a court in the state where the right is registered.

5. Licensing

Another important part of IT-regulation is licensing, which is an indispensable tool for regulators to effectively manage the complexities and challenges in this rapidly evolving field. However, it appears to be that its benefits such as mitigating risks associated with the IT sector, e. g. cybersecurity threats, data breaches, and misuse of technology are not always taken into account.

In Russia the applicable law is the Federal Law "On licensing certain types of activities" from 04.05.2011 № 99-FZ.

Article 12 lists of activities for which licenses are required. In IT-sphere these activities are the following:

1) "development, production, distribution of encryption (cryptographic) tools, information systems and telecommunications systems protected using encryption (cryptographic) tools, carrying out works, providing services in the field of information encryption, maintenance of encryption (cryptographic) tools, information systems and telecommunications systems protected using encryption (cryptographic) tools (except for the case if the maintenance of encryption (cryptographic) tools, information systems and telecommunication systems protected using encryption (cryptographic) tools is carried out for the legal entity or individual entrepreneur's own needs);

2) the development, production, sale and acquisition for sale of special technical tools designed for the covert acquisition of information;

3) activities to detect electronic devices designed for covert acquisition of information (except if these activities are carried out to meet the own needs of a legal entity or individual entrepreneur);

4) development and production of tools to protect confidential information;

5) activities for the technical protection of confidential information;

6) provision of communication services"[22].

In Sweden, according to $23 of the The Act on information security for essential and digital services providers of such services are required without hesitation notify that they are providing such services in one or several EU states.

According to chapter 3 $ 1 of the Electronic Communications Act the service of providing access to the electronic communications network both for a fee and free of charge may be provided only after an application to the supervisory authority. The use of radio transmitters on land, on a Swedish ship or in an aircraft, including an aircraft abroad, is only allowed after obtaining the appropriate permit, which gives the right to use such a transmitter in a certain frequency range.

In conclusion, in Sweden, the prevailing procedure within the IT sphere primarily revolves around a notification-only approach. Conversely, Russia adopts a contrasting regulatory framework, emphasizing the necessity of obtaining a state permit in the form of a license.

6. Main state control and supervisory authorities

Let us now delve deeper into the authorities of the state bodies responsible for overseeing information technology, including their regulatory and supervisory capacities, and their role in issuing by-laws and regulations.

Russia: The Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).

Sweden: Swedish Post and Telecom Authority (Post- och telestyrelesen) and Swedish Civil Contingencies Agency (Myndigheten för samhällskydd och beredskap / MSB).

It is worth mentioning that, in addition to its functions and powers in the field of communication and information technology, the Swedish MSB also carries out various other duties related to responding to natural disasters, crisis situations, and so

[22] Federal Law N 99-FZ On licensing certain types of activities (hereinafter referred as "Federal Law on licensing"). Art. 12. URL: https://www.consultant.ru/document/cons_doc_LAW_113658/ (In Russ.) (accessed date: 15.05.2023).

forth, essentially serving as an analogue of the Russian EMERCOM. It has it has been mandatory for swedish government agencies to report serious IT incidents to MSB since 2016. However, according to the rapport prepared by Total Defence Research institute, "during the years 2016–2018, only one third of the agencies reported IT incidents, which MSB estimates is an under-reporting" [Stenérus Dover, Bengtsson, Olsson 2020:3].

Meanwhile, other agencies also possess certain authorities in the field of our interest, thereby exercising their own regulatory powers concerning information security and personal data protection within their respective domains. For example, in addition to the Patient Data Protection Act (Patientdatalag (2008:355)) and the government decree on Patient Data Protection (Patientdataförordning (2008:360)), the Swedish National Board of Health and Welfare has issued regulations and guidelines on logging and processing personal data in the healthcare system (Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

The Swedish Post and Telecom Authority (Post- och telestyrelsen) also oversees television, radio, and postal networks, ensuring their accessibility alongside addressing information technology matters.

According to the Directive 2008:1002 with provisions on Swedish Civil Contingencies Agency (Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap t.o.m. SFS 2022:1167), the Agency "supports and guides public information security work and analyses and evaluates global trends in information security. This also includes an advisory and support role for other government agencies, regional and municipal authorities, as well as businesses and organizations in their work to prevent threats in the area of computer security".[23]

The Agency is mandated to annually report to the Government, providing an overview of incidents reported to the Agency. At the time of reporting, the Agency also receives data from the Swedish Security Service (Säpo) and the Armed Forces of the country. In addition to issuing regulations on cybersecurity, MSB also addresses emerging threats reported by government institutions. It collaborates with the armed forces in simulating cyber threats in a test environment at the Total Defense Research Institute (this project includes 800 servers that allow real-time testing of steps to counter possible attacks and has features such as Internet virtualization with geolocalized routers).

The Agency's tasks within the field of information security and secure communications include responsibility for the development and management of secure communications, advice and support in information security and responding to and preventing IT incidents.

In the field of secure communications, the Agency is responsible for developing and managing the WIS portal (part of the Swedish crisis response system where relevant authorities post information before, during and after such situations); a secure radio system for employees working in critical infrastructure and areas of public importance (e.g. police, emergency services, coast guard, etc.) and SGSI (Swedish Government Secure Intranet, a closed network for secure and encrypted communications between users in Sweden and Europe).

In addition to the above, the Agency is developing and improving secure cryptographic functions. The Swedish Armed Forces' Cryptographic System KSU (Krypto för skyddsvärda uppgifter), which consists of security material, cryptographic keys and/or activation keys, and instructions, is nationally approved for secure communications. The Agency coordinates development of secure communications in civilian government agencies.

Directive with the Provisions for the Post and Telecom Authority (Förordning (2007:951) med instruktion för Post- och telestyrelsen). § 4 focuses on the functions and competences of the Authority in the field of electronic communications.

The tasks of the Post and Telecom Authority in the area of information technology are the following.

1. "To promote safe and efficient electronic communications, including monitoring the availability of commonly used services, to facilitate access to a wide range of services for digital communications.

2. Promote and monitor the availability of broadband internet and mobile network in all parts of the country, including the establishment of pre-

[23] Directive 2008:1002 with provisions on Swedish Civil Contingencies Agency (Förordning (2008:1002) med instruktion för Myndigheten för samhällsskydd och beredskap). URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/foror dning-20081002-med-instruktion-for_sfs-2008-1002/ (In Swedish) (accessed date: 12.05.2023).

conditions for cooperation between public authorities, which could facilitate the development of a mobile network.

3. Promote effective competition.

4. Monitor developments in prices and services.

5. Carry out awareness-raising activities aimed at consumers.

6. Monitor the security situation in the field of digital communications and the emergence of possible environmental and health risks.

7. Consider permissions and obligations, establish and analyse markets and supervise and settle disputes under the Electronic Communications Act.

8. To issue regulations under the Regulation on Electronic Communications.

9. To act as a supervisory authority under Act 2016:651 on supplementary regulations to the European Parliament and Council Regulation on electronic identification and trust services for electronic transactions in the internal market and to provide support and information to public authorities and private parties with regard to trusted services.

10. Monitor the development of geographical first level domains linked to Sweden.

11. To act as a supervisory authority under the National Tier 1 Domains for the Swedish Internet Act 2006:24 and to issue regulations under the National Tier 1 Domains for the Swedish Internet Regulation 2006:25.

12. Ensure reliable electronic communications and reduce the risk of interruption, including by acquiring enablers and working to improve crisis resilience.

13. Work to improve network and information security in electronic communications, through cooperation with public authorities with special responsibilities in areas of information security, protection for national security purposes, protection of sensitive data and other actors involved.

14. Advise and support public authorities, municipal and regional authorities, companies, organizations and private persons on network security issues.

15. Act as supervisory and dispute resolution authority under the Broadband Act 2016:534 and be responsible for the Broadband Information Service under the same act.

16. To act as the supervisory authority under the Act on information security for essential and digital services"[24].

Comparing the functions outlined in the Statute of Roskomnadzor (adopted as the regulation of the Government of the Russian Federation No. 228 of March 16, 2009)[25] with the powers of the Post and Telecom Authority in Sweden reveals a set of common functions shared by both authorities:

1) state control (supervisor);

2) ensuring the sustainability, security and availability of the Internet;

3) licensing/issuing permits;

4) issuing by-laws/regulations;

5) maintaining a register of national domain names / tracking their development;

6) advice and support to other public authorities and organisations;

7) monitoring in the field of electronic communications security, counteracting threats, acquiring and providing appropriate technical means.

Roskomnadsor also issues accreditations to experts and expert organizations for content evaluation in order to ensure child information security; records, stores and processes information about advertisements distributed on the information and telecommunications network "Internet", including information about advertisers and advertisement distributors of such advertisements, advertising system operators; maintains a list of foreign entities operating in the information and telecommunications network "Internet" on the territory of the Russian Federation, and decides on the application of measures to compel such foreign entities to comply with the requirements of Russian legislation.

However, through comparing the complete lists of functions provided in two respective legal acts, it seems that the Swedish Post and Telecom Authority primarily focuses on regulatory oversight, promotion, and monitoring of electronic communications infrastructure, competition, security, and consumer awareness, while Russian Roskomnadzor focuses primarily on compliance oversight, licensing, and protection of children from harmful information within

[24] Directive with the Provisions for the Post and Telecom Authority (Förordning (2007:951) med instruktion för Post- och telestyrelsen). URL: https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/forordning-2007951-med-instruktion-for-post-_sfs-2007-951/ (In Swedish) (accessed date: 20.05.2023).

[25] Statute of Roskomnadzor (adopted as the regulation of the Government of the Russian Federation No. 228 of March 16, 2009). URL: https://eng.rkn.gov.ru/about/ (accessed date: 21.05.2023).

Russian Federation jurisdiction. Swedish Directive mentions supervisory roles under European Parliament and Council regulations, indicating international engagement, while Statute of Roskomnadzor primarily focuses on domestic regulatory functions.

In her article in "Scandinavian Studies in Law", P. Jonason addresses a significant concern regarding the influence of the Internet, social media, and search engines in various investigations, particularly by the public authorities. She highlights a case from 2013 where a Facebook post played a pivotal role in a social services decision to deny a request for the renewal of social aid.

She pointed that while the phenomenon of "administrative investigation through the search and collection of personal information on social media and the Internet at large, using search engines is not completely new, it has begun to be noticed in Sweden, in a more pronounced manner, by the Swedish Parliamentary Ombudsman (JO) in the last few years" [Jonason 2018: 272]. However, there is no relevant legislation on the topic. The social media search is not address in the Government terms of reference on the personal privacy. In her opinion, "this may, in the long run, generate citizens' distrust towards an administration they suspect is spying on them and could lead to self-restraint in the exercise of one's freedom", therefore "there is a need to regulate these kinds of practices with a legal framework capable of protecting privacy as an individual value (the privacy of the person concerned) as well as a social value (privacy as a sine qua non condition for democracy)" [Jonason 2018: 273].

The issue of using information technology as an evidence as also addressed by J. Ekfeldt, Stockholm university. He highlights that "there is a general need for future research focused on matters regarding both standards of proof for and evaluation of information technology evidence" [Ekfeldt 2016:436].

7. Standardisation

"The process of IT standardization is the dominant feature of the information industry development. The practical implementation of global concepts of IT development, namely the concept of open systems, Global Information Infrastructure, Information Society, Knowledge Society, Internet of Everything, Meta Universe, etc. is based on systematic and comprehensive IT standardization" [Sukhomlin 2022:437].

Swedish standards are the same as those in the EU. Russia uses its own GOSTs, however some of them are based on ISO/IEC standards of the International Organization for Standardization and the International Electrotechnical Commission.

The following standards are applied in Sweden:

SS-EN ISO/IEC 27001 Information security management systems – Requirements (SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav): contains requirements for information security management systems.

SS-EN ISO/IEC 27002 Code of practice for information security controls (SS-EN ISO/IEC 27002 Riktlinjer för informationssäkerhetsåtgärder): contains a list of measures to strengthen and maintain information security in the organisation.

There are considerably more applicable standards in Russia and in February 2022, the Federal Agency for Technical Regulation and Metrology (Rosstandart) published new national standards in the field of information technology:

GOST R 59898-2021 "Quality Assessment of Artificial Intelligence Systems. General provisions" contains information on the scope of application, terms and definitions, quality model, methodology and criteria for quality assessment at life cycle stages of artificial intelligence systems (AIS), general principles and procedure of AIS quality assessment, representative set of characteristics and quality indicators of AIS, and requirements to the set of input and output data for AIS testing.

GOST R 59926-2021 "Information technology. Reference architecture for big data. Part 2. Use Cases and Production Requirements" is a Russian-language adaptation of the international technical report. The document contains a detailed overview of 52 big data technology use cases, as well as technical problems identified as a result of use analyses.

It is no doubt that a balanced approach that combines the strengths of international standards with the flexibility of national ones could be the most effective. However it is crucially important to create own standards in accordance with the fast-paced development of new technologies, such as AI and big data. Similar issues are already being raised by Swedish scholars: for example C. Magnusson Sjöberg states that "the legal issues surrounding digital platforms, social media, cloud computing and AI-based services are just a few examples. How should rules on freedom of information and expression be designed and interpreted on the internet and other global networks, while respecting the right to privacy?" [Magnusson Sjöberg 2021:23]

The standards establish common terminology, methodologies, and criteria for quality assessment,

facilitating the development, implementation, and evaluation of AI systems and big data solutions, ultimately contributing to innovation, trust, and ethical use, etc. Nowadays, when the AI and its risks are on the daily agenda one can not look away and wait for the international community to agree on the applicable regulation.

8. Conclusion

The main legal acts in the IT sphere are the following:

Russia – Federal Law №149-FZ on Information, Informational Technology and the Protection of Information;

Sweden – The Electronic Communications Act 2022:482 (Lag 2022:482 om elektronisk kommunikation).

Both laws regulate the areas of information technology and contain a list of basic concepts, such as information and communication network/electronic communication network; information system operator; and information protection/network and information system security.

Through analysis conducted in this article several corresponding concepts have been identified:

Russia: *Information and Telecommunication Network* means "a technological system intended to transmit via communication lines the information further accessed using computation devices"[26].

Sweden: *Electronic communications network* means "a transmission system and, where applicable, switching or routing equipment and passive network elements and other resources which permit the conveyance of signals, by wire or by radio waves, by optical means or by other electromagnetic transmission media, irrespective of the type of information transmitted"[27] and "a device or a group of devices that are interconnected or related to each other, one or more of which carry out automatic processing of digital data through a program; or digital data that is stored, processed, retrieved or transmitted for the purpose of its operation, use, protection and maintenance"[28].

In summary, while both definitions pertain to network systems facilitating communication, the "Information and Telecommunication Network" definition appears more specific, focusing on information transmission and subsequent access. On the other hand, the "Electronic Communications Network" definition adopts a broader perspective, encompassing a variety of transmission components and methods, emphasizing signal conveyance irrespective of information type.

Russia: *Information System Operator* means an individual or a legal entity operating an Information System, including processing the data contained in its databases[29].

Sweden: *operator* "means the provider or intended provider of a public electronic communications network or an associated facility"[30].

While both definitions involve entities engaged in information-related activities, "Information System Operator" is more specific, emphasizing the operation of information systems and data processing. On the other hand, "Operator" has a broader connotation, encompassing entities providing or intending to provide public electronic communication networks or associated facilities without explicit emphasis on data processing activities.

Russia: *Protection of information* "shall represent the undertaking of legal, organizational and technical measures towards:

1) ensuring protection of information against any illegal access, destruction, modification, blocking, copying, supply, dissemination and also against other illegal actions in respect of that information;

2) observance of confidentiality of information of limited access;

3) realization of the right of access to information"[31].

Sweden: *the security of network and information system means* "the ability of electronic communications networks and services to withstand, at a given level of confidence, events that undermine the availability, authenticity, accuracy or confidentiality of the networks or services, of the data stored, transmitted

[26] Federal Law on Information. Art. 2.

[27] The ECA. Kap. 1 § 7.

[28] The Act on information security for essential and digital services 2018:1174 (Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster) (hereinafter referred as "Lag 2018:1174"). § 2. URL: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174 (In Swedish) (accessed date: 20.04.2023).

[29] Federal Law on Information. Art. 2.

[30] The ECA. Kap. 1 § 7.

[31] Federal Law on Information. Art. 16 p. 1.

or processed, or of the related services offered by or accessible through those electronic communications networks or services"[32].

In summary, Russia's focus is more information-centric, while in the Swedish legislation the main role is given to the resilience towards threats of the networks itself. Taking this into account, we can conclude that the term "protection of information" as defined in the Russian law, aims at comprehensive protection against unauthorized actions concerning information. Swedish approach is focused primarily on the ability of networks and services to withstand events, indicating a focus on the overall security and robustness of electronic communications infrastructure.

Russia: "*Critical information infrastructure* – objects of critical information infrastructure, and also electronic communication networks used for the organization of interaction of such objects.

Objects of critical information infrastructure – information systems, information and telecommunication networks, automated control systems of subjects of critical information infrastructure.

Subjects of critical information infrastructure – state bodies, public institutions, the Russian legal persons and (or) individual entrepreneurs to whom on the property right, leases or on other legal cause belong *the information systems, information and telecommunication networks, automated control systems functioning in the field* of health care, science, transport, communication, energy, the bank sphere and other spheres of the financial market, fuel and energy complex in the field of atomic energy, the defense, space-rocket, mining, metallurgical and chemical industry, the Russian legal entities and (or) individual entrepreneurs who provide interaction of the specified systems or networks"[33].

Sweden: *essential and digital services* – services provided in the following sectors: energy, transport, banking, financial market infrastructures, medical and health care, drinking water transport and distribution, digital infrastructure and digital services (online marketplaces, online search engines, cloud computing services).

As we can see, the term "critical information infrastructure" refers to the essential systems, networks, and assets that are vital for the functioning of a country's economy, security, and public welfare. The definition of the «essential and digital services» also means that these services are essential for maintaining societal functions, economic activities, and public welfare

Russia: *A computer incident* is an event of disruption and (or) interruption of the functioning of a critical information infrastructure facility, telecommunications network used to organize the interaction of such facilities, and (or) a breach of security of information processed by such facility, including as a result of a computer attack.

Sweden: *An incident* is an event that has an actual negative impact on the security of networks and information systems.

Russia: "*a search engine* is an information system that searches the Internet at the user's request for information of a certain content and provides the user with information on the page index of an Internet site to access the requested information located on Internet sites belonging to other persons, except for information systems used to perform state and municipal functions, provide state and municipal services, as well as to perform other public powers, provided by federal laws"[34].

Sweden: *internet search engine* means "a service that allows users to search virtually any website or website in a particular language by requesting any topic in the form of a keyword, phrase or other input, and returns links containing information about the requested content"[35].

In summary, while both definitions describe the functionality of internet search engines, the "Internet Search Engine" definition provides a broader description, while the "Search Engine" definition offers a more specific scope with exclusions for certain types of information systems.

The Swedish Act on Information Security for essential and Digital Services has similar concepts to the Russian Federal Law № 187-FZ About safety of critical information infrastructure of the Russian Federation. Although the list in the Russian law may seem more detailed, the areas of public activity classified as critical information infrastructure in both countries are almost identical.

[32] The ECA. Kap. 1 § 7.

[33] Federal Law № 187-FZ About safety of critical information infrastructure of the Russian Federation (hereinafter referred as "FZ-187"). Art. 2. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (in Russ.) (accessed date: 30.04.2023).

[34] Federal Law on Information. Art. 2.

[35] Lag 2018:1174. § 2.

The Swedish Post and Telecom Authority can be described as a relatively close equivalent of Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media, although a significant number of functions in the sphere of cybersecurity are under the authority of the Swedish Civil Contingencies Agency (which is similar to the Russian Ministry of Emergency Situations).

In summary, while both the Swedish Post and Telecom Authority (PTA) and Russian Federal Service for Supervision of Communications, Information Technology, and Mass Media encompass regulatory functions in the IT sphere, Roskomnadzor focuses more on compliance oversight and licensing within the Russian Federation, while Swedish PTA has a broader scope including promotion, monitoring, and security management in electronic communications with potential international engagements.

Both Russian and Swedish law criminalize computer crime. However, the Swedish Criminal Code essentially reduces the entire range of punishable computer crimes to illegal access to data and focuses specifically on breaches of data security with relatively limited penalties. Russian Criminal Code provides a broader scope which clearly means a more comprehensive approach to addressing cybersecurity threats and protecting critical information infrastructure.

Both Russia and Sweden impose fines for breaches of critical information infrastructure legislation, but in our country these are listed in the CAO (administrative liability), with different fines for individuals and legal entities. In Sweden, there is no such distinction and the fines are specified directly in the act on essential and digital services; punishment for violations of data security is limited only to fines or imprisonment for a maximum of two years.

In licensing matters, Russia adopts a permissive approach recognzing its benefits such as mitigating risks associated with the IT sector, e. g. cybersecurity threats, data breaches, and misuse of technology are not always taken into account: in order to carry out a licensed activity, a permit must first be obtained. In Sweden, a notification procedure is applied first: the law requires only that an application be submitted to the regulatory authority without delay. The licensing procedure in Sweden applies only to the use of a radio transmitter.

While Sweden primarily relies on the EU in the sphere of standartizartion, Russia has a more broad spectrum of standards and seems to prepare ground for future regulation of for example AI-based services, etc. It is of great importance to understand and establish common terminology, methodologies, and criteria for quality assessment, facilitating the development, implementation, and evaluation of such systems and solutions, ultimately contributing to innovation, trust, and ethical use, etc. Nowadays, when the AI and its risks are on the daily agenda one can not look away and wait for the international community to agree on the applicable regulation.

Sweden's reliance on implementing EU regulations has its benefits such as harmonisation, interoperability and easier market access. However, this approach may limit the country's ability to meet its specific needs and may mean additional administrative burdens associated with compliance with EU directives. Moreover, changes in EU regulations could lead to a necessity to update domestic laws, potentially causing regulatory vacuum or uncertainty, especially in such sphere as the IT sector.

In conclusion, the comparative analysis of IT regulations between Russia and Sweden reveals several key observations. Both countries exhibit similarities in their approach to defining essential concepts such as critical infrastructure, reflecting shared concerns regarding for example security issues. While Sweden aligns closely with EU regulatory framework, Russia adopts a more expansive approach, addressing emerging technological challenges such as AI. For example, existing market practices in respect of contractual liability may not be suitable for the provision of AI systems/tools [Sundberg, Tressfeldt 2022:220]

However, achieving effective IT regulation necessitates finding a balance between international consistency and national adaptability to ensure strong cybersecurity, foster innovation, and maintain regulatory flexibility in a dynamic digital environment. With that being said, a final word from S.Malmgren, associate at the Swedish law and informatics research institute: "As much as one would like all problems to be solved by a well-written legal clause, regulation goes hand in hand with the development of technology" [Malmgren 2023: 561].

References

1. Appelgren J., Zouave E. *Regelverk och krav inom området industriella informations- och styrsystem.* Stockholm: FOI. 2021. (In Swedish)
2. Efremova M.A. Criminal Liability for Unlawful Impact on the Critical Information Infrastructure of the Russian Federation. – *Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia.* 2022. № 4 (50). P. 86–92.

3. Ekfeldt J. *Om informationstekniskt bevis.* Stockholm: Stockholms universitet. 2016. (In Swedish)
4. Franke U. *Cybersäkerhet för en uppkopplad ekonomi.* Örebro universitet: Entreprenörskapsforum. 2020. (in Swedish)
5. *International Information Security: Russia's Approaches.* Ed. by A.V. Krutskikh, E.S. Zinovieva. Moscow: MGIMO-Universitet Publ. 2021.
6. Jonason P. The Use of the Internet, Social Media and Search Engines by Public Authorities in the Context of Administrative Investigations. – *Scandinavian studies in law.* 2018. № 65. P. 271–284.
7. Karzlen H., Granlund H., Wedlin M. *Operationer i cyberdomänen. En inventering av svensk forskning.* Stockholm: FOI. 2018. (In Swedish)
8. Magnusson Sjöberg C. *Rättsinformatik: juridiken i det digitala informationssamhället.* Fjärde upplagan. Lund: Studentlitteratur. 2021. (in Swedish)
9. Malmgren S. Legal tech för dataskydd: Kan teknik lösa de problem som tekniken skapat? – *Dataskyddet 50 år – historia, aktuella problem och framtid*. Ed. by D. Westman. Magnusson C. Sjöberg, Ö. Sören, D. Törngren, M. Brinnen. Stockholm: Stockholm University. 2023. P. 561–572. (in Swedish)
10. Maunsbach U., Lindskoug P. Jurisdiction and Internet in Relation to Commercial Law Disputes in a European Context. – *Scandinavian studies in law.* 2010. Vol. 56. Stockholm: Stockholm Institute for Scandinavian Law. P. 303–328.
11. Romashkina N.P., Markov A.S., Stefanovich D.V. *Mezhdunarodnaja bezopasnost', strategicheskaja stabil'nost' i informacionnye tehnologii [International Security, Strategic Stability and Information Technologies].* Moscow: IMEMO, 2020. (In Russ.)
12. Stenérus Dover A.-S., Bengtsson J., Olsson M. IT-incidenter på statliga myndigheter. – *Orsaker till utebliven rapportering.* Stockholm: FOI. 2020. (In Swedish)
13. Sukhomlin V.A. The International IT Standardization System, Its Role in the Development of the Information Industry and Its Operating Principles. – *Sovremennye informacionnye tehnologii i ITobrazovanie [Modern Information Technologies and IT-Education].* 2022. Vol. 18 (2). P. 412– 440. (In Russ.)
14. Sundberg C., Tressfeldt J. Contractual Liability when "Things Do Not Go As Planned": A Practical Perspective. – *Nordic Yearbook of Law and Informatics.* 2020–2021. Stockholm. Law Faculty, Stockholm University. 2022. P. 207–221.
15. Trenta C. The Role of Taxation in the Context of the EU Collaborative Cybersecurity Framework. – *Law and Sustainable Development: Swedish Perspectives.* Ed. by E. Kristoffersson and M. Qandeel. Uppsala: Iustus förlag. 2021. P. 97–135.
16. Vylegzhanin, A.N., Shtodina, D.D. Mezhdunarodno-pravovaja harakteristika regulirovanija onlajn-torgovli v SShA i ES [International legal characterization of e-commerce regulation in the US and the EU]. – *Vestnik Tomskogo gosudarstvennogo universiteta [Tomsk State University Journal].* 2022. Vol. 483. P. 227–239. (In Russ.).
17. Wahlgren P. The Quest for Scientific Methods: Sociology of Law, Jurimetrics and Legal Informatics. – *Combining the Legal and the Social in Sociology of Law: An Homage to Reza Banakar.* Ed. by H. Hydén , R. Cotterrell , D. Nelken & U. Schultz. Oxford: Hart Publishing. 2023. P. 227–238.
18. Wendleby, M. *Lagkommentar till NIS-lagen.* Stockholm: JP Juridiskt bibliotek. 2022. (In Swedish)
19. Wennerström E.O. *Informations- och cybersäkerhet i Sverige. Strategi och åtgärder för säker information i staten. Betänkande av NISU 2014.* Stockholm: Norstedts Juridik. 2015.
20. Westman D. Sociala medier – yttrandefrihet och Ansvar.– *Ord och rätt: Festskrift till Hans-Gunnar Axberger.* Ed. by A. Skarhed, J. Hirschfeldt, M. Ruotsi, D. Westman, S.Carlsson, Visby: eddy.se. 2020. P. 675–704. (In Swedish)

Информация об авторе

Elizaveta B. KIRILLOVA,
Attaché, MA International law, Embassy of the Russian Federation in the Kingdom of Sweden

Gjörwellsgatan 31, 112 60 Stockholm, Sweden

ebkirillova@mid.ru
ORCID: 0009-0004-4022-5279

About the Author

Елизавета Борисовна КИРИЛЛОВА,
Атташе, магистр права, Посольство Российской Федерации в Королевстве Швеция

Гьёрвеллсгатан 31, 112 60 Стокгольм, Швеция

ebkirillova@mid.ru
ORCID: 0009-0004-4022-5279