JOURNAL OF MODERN SCIENCE

6/60/2024

www.jomswsge.com

DOI: 10.13166/jms/197287

Anna Rabajczyk
Scientific and Research Centre for Fire Protection, Józefów, Poland
ORCID iD: 0000-0003-4476-8428

Monika Wyszomirska
Scientific and Research Centre for Fire Protection, Józefów, Poland
ORCID iD: 0000-0002-7780-2699

Jacek Zboina
Scientific and Research Centre for Fire Protection, Józefów, Poland
ORCID iD: 0000-0002-9436-5830

MODERN LEGISLATION REGARDING THE CHALLENGES OF 21ST CENTURY TECHNOLOGY – SELECTED ASPECTS OF LEGAL REGULATIONS AND TECHNOLOGY SECURITY

Abstract

This publication discusses legal issues related to selected areas of security, including cybersecurity, digital service security, fire safety as well as safety in the area of nanotechnology – in particular in relation to requirements concerning environmental standards, products and waste management (storage, recycling, incineration, etc.). The authors of the article analyse not only the applicable EU and national regulations, indicating the proposed areas of change, but also discuss the threats related to the use of 21st century technologies and indicate the challenges posed by new technologies in the regulatory area. By analysing extremely different substantive issues covering law, engineering and science, the authors made the same assessment of the relations between law and 21st century technology. The results of research and analyses presented by them concerning both cybersecurity and fire safety and the use of nanotechnology confirm the thesis that law is unable to keep up with the dynamic development of new technologies.

The paper uses theoretical research methods in the form of analysis of applicable EU and national regulations and the literature on the subject, as well as the results of the research work of the authors of the publication.

Keywords: *new technology law, fire safety, nanotechnologies, security of digital services, cybersecurity*

Introduction

Regardless of the political system and legal system, legal norms are always the foundation of social life and economic activity, conducted on any scale and in all areas. Without basic knowledge of regulations, it would be difficult to make rational decisions regarding everyday life, which is why legal norms should contain solutions that are adequate to the needs of citizens and the economy. In various areas of life, the process of establishing law took place gradually through the creation of new regulations, their organization or amendment in order to adapt them to current conditions (Wyszomirska M. 2023 pp. 112-118). In this publication, the authors attempt to present regulations and legal issues concerning selected areas of security, including cybersecurity, security of digital services, fire safety and safety in the area of nanotechnology – in particular in relation to both the requirements for environmental standards and products and waste management (storage, recycling, incineration, etc.).

The authors of the article analyse not only the applicable EU and national regulations, indicating the postulated areas of change, but also discuss the threats related to the use of 21st century technologies and indicate the challenges posed by new technologies in the regulatory area. The legal regulations discussed in this publication were selected due to their thematic scope, which applies to many different areas including technologies, economies, social and economic phenomena.

Security of new technologies as exemplified by the provisions of the Cybersecurity Act and the Digital Services Act

In the digital society, the development of digital technologies, artificial intelligence and data processing is clearly visible. Its most important features include: extensive use of mobile technologies and smartphones and access to new digital products and services, as well as e-medicine, new business models, and the use of data processing mechanisms to predict social processes and phenomena (Such-Pyrgiel M., Rosińska-Wielec E., 2024, p. 33). The development of new technologies and the dynamic economic development associated with them pose challenges to national and EU legislation in many legal areas, including in the area of ensuring the security of ICT systems and digital services. Due to the fact that efficient and effective operation in the cyber area is extremely important not only for national cybersecurity, but also for state security, it has become reasonable to analyse selected provisions of the Cybersecurity Act and the Digital Services Act in this publication.

Act on the National Cybersecurity System – regulatory area, principles and significance

The provisions on the organization of the national cybersecurity system are relatively new regulations, introduced into the Polish legal system by the Act of 5 July 2018 on the national cybersecurity system (consolidated text: Journal of Laws of 2024, item 1077, as amended). The aforementioned Act implements 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 EU L 194, 19.07.2016, p. 1), thereby integrating national cyber with the security systems of other members of the European Union. It is worth mentioning that through the NIS Directive, EU Member States regulated cybersecurity issues for the first time. By creating the pillars of security, in addition to the obligation of Community cooperation and sharing information, the Directive also indicated the need to establish national institutions supervising the security of entities and to create cybersecurity systems that would secure individual sectors of the economy.

The response to the EU recommendations is the Act on the National Cybersecurity System, which through successive amendments covers an increasingly wider circle of obliged entities. In accordance with Art. 1 sec. 1, the subject of the Act is to define the organization of the national cybersecurity system and the tasks and obligations of entities included in this system, the method of exercising supervision and control in the scope of the application of the provisions of the Act, as well as the scope of the Cybersecurity Strategy of the Republic of Poland. The Act contains provisions that regulate, among others:

- principles of identification, registration and obligations of key service operators;
- obligations of digital service providers;
- tasks of CSIRT MON, CSIRT NASK and CSIRT GOV;
- principles of sharing information and processing personal data;
- authorities competent for cybersecurity.

Technology is an integral part of social life. The widespread use of computers and the development of information and communication technologies have made people dependent on this technology in many ways (Florek I.B., Eroglu S.E. 2019, p. 27). The national cybersecurity system aims to ensure cybersecurity at the national level, including the uninterrupted provision of key services and digital services, by achieving an appropriate level of security of information systems used to provide these services and ensuring incident handling (Article 3 of the Act). For the purposes of cybersecurity, a catalogue of concepts was created, which the legislator defined in detail in Article 2 of the Act, and in this publication the authors will only cite those definitions that are necessary to discuss the subject of the article.

In the statutory sense, **cybersecurity means the resistance of information systems to activities that violate the confidentiality, integrity, availability and authenticity of processed data or related services offered by these systems**. A cybersecurity threat should be understood as a potential cause of an incident, i.e. an event that has or may have an adverse effect on cybersecurity. Assigning it a critical degree means that its occurrence will cause significant damage to public safety or order, international interests, economic interests, the operation of public institutions, civil rights and freedoms or human life and health. If the incident is serious, then there is a fear that it causes or may cause a serious reduction in quality or interruption of the continuity of service provision. The tools used for security include proper risk assessment and incident management through its handling, finding connections between incidents, removing the causes of their occurrence and developing conclusions resulting from the handling of the incident.

The entities covered by the cyber system include, among others:

1. key service operators;
2. digital service providers;
3. CSIRT MON (Computer Security Incident Response Team operating at the national level, led by the Minister of National Defense);
4. CSIRT NASK (Computer Security Incident Response Team operating at the national level, led by the Scientific and Academic Computer Network – National Research Institute);
5. CSIRT GOV (The Computer Security Incident Response Team led by the Head of the Internal Security Agency, operates as a CSIRT Team at the national level in Poland);
6. public finance sector entities referred to in art. 9 items 1-6, 8,9,11 and 12 of the Public Finance Act (Public Finance Act, 2023);
7. research institutes;
8. National Bank of Poland, Bank Gospodarstwa Krajowego, Office of Technical Inspection, Polish Air Navigation Agency, Polish Accreditation Centre, National Fund for Environmental Protection and Water Management and provincial funds for environmental protection and water management;
9. other entities listed in art. 4 of the Cybersecurity Act.

The legislator excludes the application of the provisions of the Act to telecommunications entrepreneurs referred to in the Electronic communications law (Journal of Laws of 2024) in the scope of requirements concerning security and incident reporting, entities performing medical activities – created by the Head of the Internal Security Agency or the Head of the Intelligence Agency, as well as trust service providers who are subject to the requirements of Article 19 of the Regulation of the European Parliament and of the Council on electronic identification and trust services (Regulation (EU) No 910/2014. This is a narrow group of *excluded* entities, because the role of the cybersecurity regulations is to guarantee the highest possible level of network security. For this purpose, the statutory provisions indicate, among other things, what the composition of the critical infrastructure should be and impose on entities of the national cybersecurity system tasks related to both incident handling and preventive actions in these entities. For example, **key service operators** are required to implement a security management system in the information system used to provide the service by, for example, estimating the risk of an incident and managing this risk, implementing proportionate technical and organizational measures (taking into account the latest state of knowledge), collecting information on network threats; applying measures to prevent and limit the impact of incidents on the security of the information system used to provide services. **Digital service providers** also have obligations to detect, record, analyse and classify incidents.

In accordance with Annex No. 2 to the Act on the National Cybersecurity System, to which Article 17 section 1 of the aforementioned Act refers, a digital service is considered to be:

- Online marketplace – a service that enables consumers or entrepreneurs to conclude contracts electronically with entrepreneurs on the website of the marketplace or on the website of an entrepreneur who uses the services provided by the online marketplace;
- Cloud computing service – a service that enables access to a scalable and flexible set of computing resources for shared use by multiple users;
- Internet search engine – a service that enables users to search for all websites or websites in a given language by means of a query by entering a keyword, phrase or other element, presenting as a result links relating to information related to the query.

Digital service providers, like operators of an essential service, are therefore obliged to implement measures ensuring the cybersecurity of information systems and facilities, using the latest state of the art and complying with international standards.

Another group of entities on which the Cybersecurity Act imposes obligations to protect the security of systems are **public entities**, whose obligations are not limited solely to incident management in a given public entity, but have a nationwide scope. The tasks of CSIRT MON, CSIRT NASK and CSIRT GOV include, among others:

1. monitoring cybersecurity threats and incidents at the national level;
2. conducting dynamic risk analysis;
3. issuing messages on identified cybersecurity threats;
4. classifying incidents;
5. cooperation with sectoral cybersecurity teams in coordinating the handling of serious incidents;
6. forwarding to other countries, including European Union Member States, and receiving from these countries information on serious incidents and significant incidents;
7. joint development and submission to the minister responsible for computerization of parts of the Report on National Security Threats;
8. participation in the CSIRT Network consisting of representatives of the CSIRTs of the European Union Member States, the CSIRTs responsible for the European Union institutions, the European Commission and the European Union Agency for Network and Information Security (ENISA).

In accordance with the national cybersecurity system, entities involved in the system, including the Minister of Digital Affairs and key service operators, are required to ensure the continuity of operation and security of the state in their actions. The act in question is of great importance not only for the cybersecurity of public order or the infrastructure of financial and telecommunications markets, but also for online trading platforms and economic entities of particular importance for defence.

Taking the above into account, it should be emphasized once again that the globalization of the services and supply market, which is co-created by the global

telecommunications network, creates threats of cyberattacks, and these in turn give rise to the need to ensure the security of systems. Effective combating of cybercrime would not be possible without the cooperation of EU members and many countries outside the Community, as well as the involvement of private entities, including primarily Internet service providers. In order to secure critical systems and data against unauthorized access, entrepreneurs and public entities introduce various types of strategies, procedures and technological solutions to protect digital resources from hacking. This diversity of processes also poses a serious challenge to the legislator, who creates regulations protecting network security. When assessing the national cybersecurity act in this context, it should first be noted that the NIS Directive only indicated the direction of action, leaving the Member States considerable freedom in shaping the regulations. In the absence of international standards in the field of network protection, it can be argued that the national act in force since 2018 has created an optimal model of the country's cybersecurity system. Amendments to the act show that the dynamic development of technology will also force changes in the regulations, and keeping up with these changes in order to secure critical systems will certainly be a serious challenge for the modern legislator.

Digital Services Act (DSA) – the European Parliament's proposal to standardise the procedure for removing illegal content from the internet

The use of new technologies is currently linked to large platforms and internet search engines, which is why the security of 21st century technology and its users depends to a large extent on online security.

In response to the need to create a safer digital space, EU countries have developed standards included in Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act). This regulation has already covered large platforms and internet search engines since 25 August 2023, and since 17 February 2024 the regulation has also become applicable to all intermediary service providers (e.g. social networking sites, hosting providers, e-commerce platforms).

The creation of a single set of EU-wide regulations resulted from the need to streamline and coordinate the regulatory activities of the Member States and to establish authorities supervising compliance with the regulations.

The Digital Services Act (DSA) contains provisions that protect all internet users in the European Union, both in terms of illegal goods, content or services and their fundamental rights, such as freedom of expression, freedom of thought, freedom of opinion without manipulation and freedom of information.

In order to protect the safety of internet users, the **Digital Services Act** introduces, among others:

1. a ban on the use of minors' data and sensitive personal data by internet platforms for profiling purposes for advertising purposes;
2. a ban on profiling users based on specific categories of data, such as sexual orientation, ethnic origin or religious beliefs.
3. control over the posting of content that spreads hatred, violence or child pornography;
4. an obligation for platforms to provide information on content moderation and the operation of algorithms, which will give the user knowledge of how content is assessed and how a given internet platform works;
5. implementation by platforms of procedures that will ensure the transparency of internet advertising;
6. the right of the user to appeal against the platform's decisions;
7. supervision by the European Commission of very large internet platforms and search engines – VLOPs (largest platforms such as Facebook, YouTube, Instagram, Twitter (X) or TikTok, with more than 45 million monthly active users in the EU) and VLOSEs (largest internet search engines such as Bing and Google Search, that provide their services to 45 million or more average monthly active users in the EU);
8. supervisory powers of the Commission, analogous to antitrust regulations, including the right to impose fines of up to 6% of global revenue;
9. the obligation for Member States to appoint coordinators for digital services, whose tasks will include supervising the compliance of services in a given country and participating in the EU cooperation mechanism.

The assessment of the effectiveness of the new regulations will of course only be possible after testing in practice the solutions proposed in the DSA provisions. It is currently important to analyse the correlations between the European Parliament regulation on digital services and other regulations, such as the E-commerce Directive 2000/31/EC (OJ L 178, 17.7.2000) and the General Data Protection Regulation (Personal Data Protection Act 2018, Journal of Laws of 2019, item 1781).

The E-commerce Directive specifies requirements for online service providers in terms of transparency of information, establishes rules for drawing up electronic contracts, and strengthens the role of self-regulation and administrative cooperation between Member States. The Directive, by creating a framework for e-commerce, therefore aims to reduce discrimination against entities (consumers and businesses) that access content or purchase goods and services online in the European Union. It should be noted that the Digital Services Act does not replace the E-commerce Directive, but extends, supplements and modernises it.

The Digital Services Act does not replace the GDPR either, but proposes additional provisions ensuring the highest level of data protection. The development of online platforms and the ever-increasing level of use of the Internet force the legislator to take legislative action in order to best secure the rights of consumers and businesses. In order to meet these needs, in the case of processing personal data for advertising purposes, dual restrictions resulting from both the GDPR and the Digital Services Act are imposed on online platform providers. Regardless of the obligations set out in the GDPR, the Digital Services Act prohibits the creation of advertisements that use user profiling based on data such as ethnic origin, sexual orientation or religious beliefs. It also prohibits advertisements that use sensitive data or data of minors.

The rapid development of the Internet poses a serious challenge to modern legislation not only due to the very broad regulatory area, but above all due to the pace of development of information technologies. According to the authors, as a result of the analysis of EU legal regulations, it can be stated that the Digital Services Act makes a significant contribution to the creation of digital regulations. When analysing EU regulations on digital services, it is also necessary to ask how the Polish legislator will implement these principles into national regulations. Work is currently underway on an amendment to the Act on the provision

of services by electronic means (Act, Journal of Laws of 2024, item 1513), which is to implement the provisions of EU Regulation 2022/2065. Among other things, the designation of a body acting as a coordinator for digital services, the introduction of national procedures for granting the status of a trusted whistleblower and verified researcher, or the definition of the principles of control and imposition of fines have been transferred to the national level. It can be assumed that as part of the implementation work, the Act on the provision of services by electronic means will be amended first, which does not mean that other legal acts that contain references to the above will also be amended. the Act and relevant sectoral regulations will also require changes.

Analysis of legislation in the field of nanotechnology

The development of new technologies, including nanotechnology, currently represents great opportunities, but at the same time it can also generate threats and challenges. Nanotechnology, as a dynamically developing field of science and knowledge, creates not only new opportunities, but at the same time it is associated with the emergence of completely new threats related to the increasingly common use of nanosubstances (Rabajczyk A, Wyszomirska M, Zboina J., 2024 pp. 63-84). Nanotechnology refers to the area of particles with sizes ≤ 100 nm, however, there are several definitions of nanotechnology and nanotechnology products, which are often created for specific purposes (SCIENTIFIC COMMITTEE ON EMERGING AND NEWLY IDENTIFIED HEALTH RISKS (SCENIHR), SCENIHR/002/05). According to the definition proposed by the British Royal Society and the Royal Academy of Engineering in 2004 (Royal Society and the Royal Academy of Engineering 2004) the nanoscale ranges from the atomic level, from about 0.2 nm to about 100 nm. he British Standards Institution in the Publicly Available Specification (PAS) glossary related to nanoparticles (BSI 2005), he following definitions have been proposed for various concepts, including:

- nanoscale: having one or more dimensions of the order of 100 nm or less;

- nanoscience: the study of phenomena and manipulation of materials at the atomic, molecular and macromolecular scale, where the properties are significantly different from those at larger scales;
- nanotechnology: the design, characterisation, production and application of structures, devices and systems by controlling shape and size at the nanoscale;
- nanomaterial: a material with one or more external dimensions or an internal structure that can exhibit new properties compared to the same material without nanoscale features;
- nanoparticle: a particle with one or more dimensions in the nanoscale;
- nanocomposite: a composite in which at least one of the phases has at least one dimension in the nanoscale;
- nanostructured: having a structure in the nanoscale[9].

According to the 2022 European Commission Recommendation (Recommendation 2022/C 229/01), a nanomaterial means a *"natural, incidental or manufactured material consisting of solid particles that occur either alone or as identifiable constituent particles in aggregates or agglomerates, and in which at least 50% of such particles in the number size distribution meet at least one of the following conditions:*

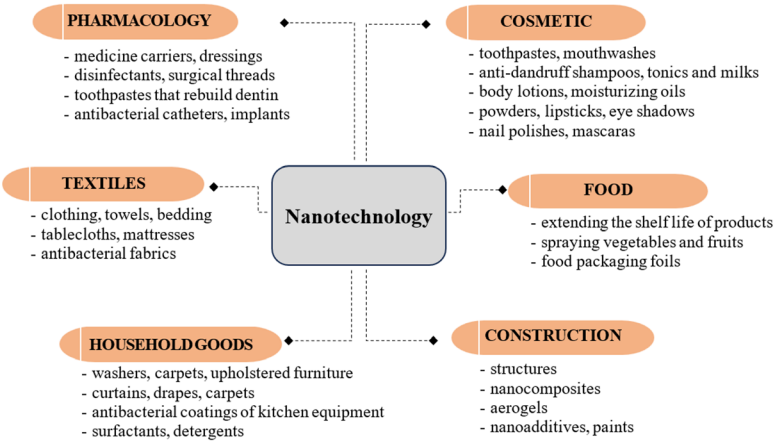
a. *at least one external dimension of the particle is in the range 1-100 nm;*
b. *the particle has an elongated shape, such as a rod, fibre or tube, where two external dimensions are less than 1 nm and the other dimension is greater than 100 nm;*
c. *the particle has a plate-like shape, where one external dimension is less than 1 nm and the remaining dimensions are greater than 100 nm.*

*When determining the number size distribution, particles with at least two orthogonal external dimensions greater than 100 μm may be disregarded. However, a material with a volume specific surface area of < 6 m^2/cm^3 is not considered a nanomaterial" (*Project Report Series on Chemical Accidents. ENV/CBC/MONO(2022)19, 2022, No. 34).

It should be noted that this understanding of a nanomaterial has been in force only since 2022, and until then the definition contained in the

Commission Recommendation of 18 October 2011 specifying the definition of a nanomaterial 2011/696/EU and the definitions of a nanomaterial in sectoral regulations were in force – which often caused interpretation problems. Additionally, in the literature devoted mainly to aerosols, including in relation to air pollution or inhalation toxicology, there are such terms for nanoparticles as ultrafine, fine or conventional, which can also be misleading. An unambiguous indication that a given solution concerns a nanosubstance is important, among other things, due to the fact that these substances are characterized by different properties than their macro counterparts. The large surface area combined with a very low mass, characteristic of nanostructures, allows for a wide range of applications in various areas of industry, including construction, mechanical, electrical, food, pharmaceutical and household products (Figure 1).

Figure 1: *Examples of nanotechnology applications in selected industrial areas*



Source: own preparation.

According to Janković and Plata (Janković N., Plata D. 2019), who published data presenting the production volume of selected 25 nanomaterials, the most produced nanoparticles are silicon dioxide (n-SiO_2), titanium dioxide (n-TiO_2), (nano) clays, zinc oxide (n-ZnO) and aluminum oxide (n-Al_2O_3). Considering the application and rate of utilization of nanoparticles, it has been estimated

that by 2025 the annual global production of titanium dioxide nanoparticles alone will reach 2.5 million. (Project Report Series on Chemical Accidents. ENV/CBC/MONO(2022)19, 2022, No. 34). It should be noted that the accuracy of the data on production volume is limited, because these data depend mainly on voluntary reporting by companies.

Taking the above into account, both the European Union and individual countries or organizations such as the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) or the Scientific Committee on Consumer Products (SCCP), responsible for shaping the law in the field of safety and labor law, are developing appropriate requirements and recommendations. In the case of the EU, provisions relating to nanotechnology have been included in many successively updated documents, including (among others):

1. Resolution of the European Parliament of 24 April 2009 on regulatory aspects of nanomaterials (2008/2208(INI);
2. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorization and Restriction of Chemicals (REACH);
3. Directive 98/8/EC of the European Parliament and of the Council of 16 February 1998 concerning the placing of biocidal products on the market, together with Regulation (EU) No 528/2012 of 22 May 2012 concerning the making available and use of biocidal products;
4. Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work and its daughter directives;
5. Directive 2001/95/EC of the European Parliament and of the Council of 3 December 2001 on general product safety;
6. European Parliament Resolution of 10 July 2020 on the Chemicals Strategy for Equivalence (2020/2531(RSP)) (2021/C 371/11);
7. Decision (EU) 2022/591 of the European Parliament and of the Council of 6 April 2022 on a General Union Environment Action Programme to 2030.

One of the main documents directly related to nano-substances is the REACH Regulation (Registration, Evaluation, Authorisation and Restriction of Chemicals), according to which all substances falling within the scope of

the REACH Regulation must be registered in order to be legally manufactured in the EU or imported into the EU. As part of the registration, manufacturers or importers are required to submit information on the impact of nano-substances on human health and the environment, as well as to estimate exposure throughout the life cycle (this depends on the quantity introduced to the market). If the substances have hazardous properties, the Classification, Labelling and Packaging Regulation (CLP) requires these substances to be notified to the European Chemicals Agency (ECHA) and appropriate labelling and packaging in such a way that it is possible to use them safely (EUON 2024, REGULATION (EC) No 1907/2006, OJ L 396 30.12.2006, p. 1) REACH registration should provide information that clearly defines how safety issues of nano-substances have been addressed, including what measures are necessary to adequately control potential risks. The main area of interest of the legislator is primarily issues related to the safety of products in which nano-substances are used, such as medicines, materials, packaging, biocidal products, plant protection products, cosmetics, toys, food or electronics. Therefore, in addition to the REACH and CLP regulations, sectoral legislation also applies in the European Union. For example, on 14 March 2024, the legal provisions on the use of nano-substances in cosmetic products were amended. By way of Commission Regulation (EU) 2024/858 amending Regulation No. 1223/2009 with regard to the use in cosmetic products, nanosubstances such as styrene/acrylic copolymer, sodium salt of styrene/acrylic copolymer, copper, colloidal copper, hydroxyapatite, gold, colloidal gold, gold with thioethylamine and hyaluronic acid, acetylheptapeptide-9 with colloidal gold, platinum, colloidal platinum, acetyltetrapeptide-17 with colloidal platinum and colloidal silver have been banned (EU Commission Regulation 2024/858, Dz.U. L, 2024/858, 15.3.2024). The regulations introducing a ban on the introduction of cosmetic products that do not meet the new requirements will come into force on 1 February 2025. In turn, from 1 November 2025, a ban on making such cosmetics available on the EU market will also come into force. However, it should be noted that in the case of compounds such as styrene/acrylic copolymer (nano) and sodium salt of styrene/acrylic copolymer, the ban is a consequence of the lack of sufficient data to assess possible toxicity. EU legislation is constantly trying to regulate areas where nano technologies are used. In the case of nano-substances that

pose a risk to the environment, workers or consumers, as for other forms of substances, the general principles apply, which are defined by:

Council Directive 76/768/EEC of 27 July 1976 on the approximation of the laws of the Member States relating to cosmetic products together with EU Regulation (EC) No 1223/2009 of 30 November 2009 on cosmetic products

Regulation (EC) No 178/2002 of the European Parliament and of the Council of 28 January 2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety

Regulation (EC) No 1333/2008 of the European Parliament and of the Council of 16 December 2008 on food additives

Directive 2000/13/EC of the European Parliament and of the Council of 20 March 2000 on the approximation of the laws of the Member States relating to the labelling, presentation and advertising of foodstuffs

Regulation (EC) No 1830/2003 of the European Parliament and of the Council of 22 September 2003 concerning the traceability and labelling of genetically modified organisms and the traceability of food and feed products produced from genetically modified organisms

Regulation (EC) No 258/97 of the European Parliament and of the Council of 27 January 1997 concerning novel foods and novel food ingredients

Community legislation in the field of the environment, in particular:

- Directive concerning integrated pollution prevention and control,
- Directive establishing a framework for Community action in the field of water policy,
- Directive on waste.

In the case of protecting employees from exposure to carcinogenic or mutagenic factors at work, a directive is in force, which establishes general guidelines, principles, obligations of the employer and employee and indicates the permissible time of exposure to pathogenic factors. It is worth noting that the activities of the European Union in combating the causes and negative effects of air pollution with carbon dioxide are largely coordinated with the activities of international organizations, including the UN. (Sitek M. 2023, p. 18). However, there are no precise regulations regarding nanosubstances.

This is important because the presence of nanoparticles in the workplace is related not only to the production of nanosubstances or their use in production. It should be noted that nanoparticles may have unintentional emissions from various sources, including from all types of work related to the design of nanoparticles, development and production by humans for the purpose of application. Emissions may occur, for example, at the stage of developing a method for the synthesis of nanosubstances, the production of nanosubstances, including individual elements of the production line, as well as during the use of products containing a nanosubstance. The presence of metal nanoparticles in the workplace is influenced by various types of processes that result in the unintentional formation of nanoparticles, such as welding, soldering, welding, vulcanization, plasma cutting, grinding, cutting, drilling, polishing, spraying paints containing nanosubstances, cleaning devices of nano dimensions or burning fuels in diesel engines, operating electric motors, copiers, faxes and printers. The results of the studies show that the highest concentrations of nanoparticles occur in rooms related to the metal industry or, for example, construction (Rabajczyk A., Zielecka M., Hopke P., Porowski R., 2020). It was also found that depending on the industry, the chemical composition of particles is extremely diverse (Rabajczyk A., Zielecka M., 2020, pp. 48-50). In the case of office spaces, the main source of nanoparticle accumulation are primarily ventilation systems or carpets spread on the floors, but also electronics, including computers, in which nanoparticles are used. In the case of places where metalworking is carried out, the main source is dust generated during welding and grinding processes. In the case of places where woodworking is carried out, the source are substances used as impregnates, varnishes or dust generated during abrasion processes. The presence of nanoparticles and their emission in the workplace means that the priority is to ensure the safety of both employees and the technologies used. However, it should be noted that there are no systematic or mandatory reporting systems that would allow for the identification of failures related to nanosubstances, which means that the above list cannot be considered exhaustive and complete. The European Union Observatory for Nanomaterials (EUON) provides information on existing nanomaterials on the EU market (EUON) According to the data presented, France, Norway, Denmark, Sweden and Belgium have taken

national initiatives to obtain more comprehensive information on nanomaterials from companies than is required by the EU. Their national regulations differ in terms of the information actually requested from companies and the scope of exemptions and information available to the public. Belgium, France and Denmark have separate inventories for nanomaterials, while Norway and Sweden have included a section dedicated to nanomaterials in their existing product registers. For example, in France, a national decree on the mandatory notification of nanomaterials has been in force since 1 May 2013 (Declaration Exercice 2024), while in Belgium, a Royal Decree on the placing on the market of substances produced in nanoparticle form has been in force since 1 January 2015 (nanoregister, Belgia 2024), France requires information on, among other things, the company and users of nanomaterials, physicochemical data and (eco)toxic properties of the nanomaterial, annual turnover, and the use of the substance. Considering the fact that nanotechnology has been widely used in various sectors of the economy for several decades, these requirements are still limited and insufficient. They do not fully take into account the risks that nanotechnologies pose to employees at work, because the main recipients of the introduced legal requirements are consumers and manufacturers. It should be noted that the applicable regulations require employers to assess and control the risks posed by chemicals at work, including nanomaterials, and to take action to eliminate or reduce the risk (EUON). The problem, however, is the lack of appropriate standards and legal requirements dedicated directly to nanotechnology. It should be remembered that nanosubstances are characterized by different properties than their counterparts in the nano area, which is why it is so important to develop requirements for this area. Another important issue is the lack of awareness of the risk resulting from the presence of nanoparticles in the work environment and their emission during work. (Rabajczyk A., Wyszomirska M., Zboina J.,2024, ss. 63-84). There is still insufficient knowledge about the threats that nanoparticles may pose (e.g. explosion hazard) and reliable information for employers and employees, which significantly affects safety in the workplace.

Another important issue that requires analysis is the presence of nano-substances in the environment, understood not only as a consequence of natural processes, but primarily as a result of human activity. For example, nano-substances can be emitted with sewage to surface waters or soils, and they can enter

sewage from many sources, including those related to hygiene, cleaning and repair of installations or a given facility, as well as directly at points determined by the technology used, including, for example, preparation of solutions and emulsions, bathing, dyeing, electrolysis, waste leachates, water purification. However, in the regulations relating to the degree of removal or reduction of pollutants in sewage, there are no guidelines relating directly to nano-pollutants – purification processes refer primarily to the total concentration of a given pollutant, without taking into account *nano* forms. (Rabajczyk A, Zielecka M., 2020, ss. 48-51). It should also be noted that there is still no data on the natural concentration of nanoparticles in the environment that would allow for the creation of even soft law (guidelines, principles, recommendations). An additional difficulty is the fact that many nanosubstances produced by humans do not occur naturally in the environment. Their presence is therefore the result of dedicated syntheses, which may be an indicator of the degree of contamination by human activity.

When analysing the regulations dedicated to nanotechnologies, one cannot ignore Decision 2022/591 on the General Union Environment Action Programme to 2030 (Dz.U. L 114 z 12.4.2022, p. 22–36). The above-mentioned regulation indicates that in order to achieve the priority objectives, both the European Commission and the Member States, regional and local authorities and stakeholders should assess the impact of nano on health and the environment, including climate and biodiversity, and promote chemicals and materials that are safe and sustainable at the design stage.

Intensive research allows for gradual filling of gaps in the area of nano-substances' behaviour in the environment. However, this is insufficient due to the lack of environmental standards directly related to nano-substances, taking into account not only the size of particle grains, but also, for example, surface structure, grain shape, composition, oxidizing/reducing properties or biochemical activity. According to the recommendations indicated by EUON, the starting point may be physicochemical properties, such as water solubility. In the case when a readily soluble substance is released into the environment, the environmental properties in the solution of this substance should be assessed regardless of whether we are dealing with a substance in the nano-range. If the nano-substance is readily soluble, then in the case of

inorganic substances, existing information on its mass form can be used to assess its nanoform as well (EUON).

The Organisation for Economic Co-operation and Development has published a number of guidance documents, including on sample preparation and dosimetry for testing. Work is also underway to develop regulatory tools for assessing and managing the risks of nanomaterials, including addressing environmental risk assessment and identifying alternative testing strategies. Guidelines and handbooks are under preparation, containing recommendations to support a Life Cycle Assessment (LCA) approach to decision-making on nanomaterials (Nanotechnology Regulation, CCOS 2024). Nano-substances can be released at any stage of the cycle, both at the initial stage, which is the development of a given substance, and at the end of the cycle – as waste. The European Directive on the Landfill of Waste (1999/31/EC) contains requirements for the construction and operation of a landfill, including, among others, the discharge and treatment of leachates or the collection of gases from landfills. However, it does not take into account issues related to *nanowaste*, i.e. waste that contains substances with dimensions in the nano range. The problem is important because *nanowaste* is created in every aspect of our lives. They have a very diverse structure and are introduced into the waste stream along with other products that do not contain nanostructures. Additionally, the release of metal nanoparticles into the environment can take place at virtually all stages of the waste management system, including collection, recycling, incineration or storage. (Rabajczyk A, Zielecka M., 2020, pp. 48-51).

Another significant problem is the issue of using sewage sludge as a method of disposing of *nanowaste*. According to estimates, 90–95% of nanosubstances contained in sewage accumulate in the sludge, while sewage sludge is managed in various ways. Nanosubstances, such as silver, gold or iron nanoparticles contained in sewage sludge, can then be released during combustion or migrate to soil, disrupting natural processes occurring in this element of the environment (Mrowiec B., 2016, pp. 593–596). Legal regulations do not standardize the amount of individual nanosubstances in sewage sludge and the processes that can be used to dispose of sludge. The lack of a range of permissible concentrations in the legislation and tools for testing and verifying the amount of nanoparticles in the environment means that uncontrolled

amounts of substances from the nano area are introduced into the environment, contributing to an increase in threats to human life and health and the quality of the environment. Selected issues related to the use of nano indicate the need for cooperation between many groups in order to develop legal regulations to ensure the safe use of nanotechnology. The provisions of EU law discussed in this article do not, of course, satisfy all legislative needs in the field of nano, but nevertheless they define the principles and guidelines so important for the safe use of 21st century technologies.

Legal regulations in the area of security

The need to create appropriate regulations in the area of security is an issue that is often raised and discussed. Over the years, it has been subject to evaluation and improvement due to the goal of ensuring security. The research results presented in this publication and the conclusions formulated on their basis, using the example of areas such as cybersecurity and nanotechnology security, are a representative example of the needs and challenges in the field of legal regulations. Referring to previous own research (Zboina J. 2020), it is justified to claim that law is a key foundation necessary for the implementation of new technologies. Legal regulations can promote innovations by facilitating the use of new solutions, they can be neutral or even prevent their implementation. The lack of such regulations is only seemingly neutral. As a rule, however, this is not a favorable situation if the implementations concern the area of security. Insufficient legal regulations in this area result in a formal obligation to ensure broadly understood security without any guidance on how to achieve this. The reference point for requirements and conditions for the use of new and innovative products, systems or solutions, including new technologies, are very often products already in use, for which regulations, requirements and technical standards exist and are already enforced. They take the form of detailed legal regulations and technical requirements, described appropriately in product standards, documents or directly in the regulations. In addition, in some countries, additional, non-legal industry requirements, as well as requirements set by insurance companies, also play an important

role in the area of fire safety. In the opinion of many experts, including the authors of this publication, the best situation for the development of innovation and implementation of new technologies is a situation in which there is an appropriate legal environment and industry practice that is conducive to the implementation of new products and technologies. The most unfavourable case occurs when, in addition to the lack of *facilitations*, there are effective formal and informal barriers that prevent the creation and introduction of new solutions, despite market demand. Therefore, currently and probably in the near future, work on solutions beneficial to the development of technology will be undertaken both in the field of science and in commercial activities.

There is no doubt that law is one of the key elements of creating and developing innovation, as well as applying new technologies. The same conclusions were formulated in the recent past in the context of predicting and forecasting the development of drone technologies in Poland in 2017 (Kosieliński S., 2017), defining at that time the lack of legal regulations regarding conducting flights (missions) as the main barrier and obstacle to the mass adoption of this technology in various applications – from use in rescue or transport, through geodetic and film services, agricultural applications, and ending with the vision of delivering pizza using unmanned aerial vehicles.

The security of new technologies is a priority, and legislation is a tool for achieving this goal. Requirements for the technology of emerging products, the conditions of their use and requirements for manufacturers, including their responsibility for products and services, are an area of building trust between different parties. Security and the trust it builds are the basis for the development of any technology. But what about the facts discussed by the authors of the article confirming the thesis that the creation of law is becoming more detailed, complex and extended in time, while technological development is still accelerating? Analyzing, in the context of security, the current conditions for the implementation of new technologies and innovations, it can be predicted that in the near future the state of discrepancy between the needs in the scope of legal regulations concerning the use of new technologies and their development will deepen. The above statement is justified primarily by the fact that the law is being created for an increasingly longer time, legislative techniques are evolving and regulations are becoming more complicated, while on the other hand,

technological development is still accelerating, providing new opportunities and, of course, also creating threats. Trust in new products, solutions and technologies, including in relation to their declared parameters, intended scope of application, effectiveness of operation, reliability, ergonomics and safety is the basic condition determining their use. This trust is particularly important in the case of safety products, which include active and passive fire protection. They have specific, dedicated properties that allow the design of intended functions and functionalities in fire protection. This goal is achieved by establishing formal (legal), industry requirements and insurance standards. The challenge concerns both ensuring the properties of products used in fire protection, i.e. fire brigade equipment and equipment and active and passive fire protection used in buildings, as well as shaping trust in products used in these facilities. Conformity assessment and approval processes for products used in fire protection are important elements of the fire safety policy of each country. The approval processes for products introduced into use and used by fire protection units are an important tool for ensuring the necessary safety for rescuers and rescued persons, as well as fire safety in buildings.

Another challenge is the proper functioning of this system and its adaptation to changing needs. The best products, but incorrectly designed, installed and operated, do not allow achieving the goals of fire protection or, in a broader sense, the goal of safety. It should also be emphasized that fire protection systems and safeguards evolve in the face of the challenges posed by new technologies. An example of this is the dedicated fire protection conditions created for the intensively developing electromobility (CNBOP-PIB, Wytyczne 2024), energy and renewable energy sectors (CNBOP-PIB, Ocena ryzyka pożarowego 2021). Thus, it is justified to conclude that effective implementation of new technologies requires appropriate legal regulations that contain requirements for their safety, building trust in them and providing a basis for development. However, in many economic areas there is a lack of regulations, which is a hindrance or even a significant barrier to development. Regardless of the previously discussed legal aspects influencing the development of technology, local or national conditions dedicated to individual regions, countries or cultures are also important for the safety of innovative solutions. This aspect is important for implementing new solutions that are already in operation in other countries

and that we intend to implement in Poland. Omitting this particular aspect or not taking it into account enough may result in unsatisfactory implementation results or even prevent the introduction of innovative solutions.

Conclusion

Law is an area without which it is difficult to imagine the functioning of the state as an organized form of organization of society and all kinds of activities that it generates. The development of 21st century technologies poses enormous challenges to the modern legislator, because the dynamics of new technologies prevent the traditional normative model from fully realizing its goals (Wyszomirska M., 2024, pp. 96-110) among the activities requiring legal regulations are also new technologies.

The authors of this publication, examining extremely different substantive issues covering law, engineering and science, made the same assessment of the relations between law and 21st century technology. The results of research and analyses presented by the authors regarding both cybersecurity and fire safety and the use of nanotechnology confirm the thesis that the law is unable to keep up with the dynamic development of new technologies. According to the authors, the law-making process prevents the effective creation of regulations supporting new technological solutions.

The increasingly rapid pace of development, with unchanged legislative techniques, deepens the discrepancies between legislation and new technologies. This situation does not mean, however, that we should give up regulating innovative solutions altogether. Soft law is becoming an alternative to statutory acts, in the form of, among others, technical assessments, expert opinions, national standards or industry guidelines in the field of safety. The use of soft law and abstract/general statutory provisions will enable, on the one hand, the creation of a legal framework for action, and on the other hand, will ensure the safe implementation of new technologies. The safety of introducing new solutions to the market is a priority issue, therefore, the modern legislator and scientific and business communities face the challenge of creating regulations supporting 21st century technologies.

References

Act of 27 August 2009 on public finances. Journal of Laws. 20241.530, consolidated text.

Act of July 12, 2024, Electronic Communication Law. Journal of Laws. 2024. 1221, consolidated text.

Act of 10 May 2018 on the protection of personal data. Journal of Laws 2019. 1781, consolidated text.

Act of 18 July 2002 on the provision of electronic services. Journal of Laws. 2024. 1513, consolidated text.

British Standards Institution (BSI). (2005).Vocabulary – Nanoparticles, Publicly Available Specification, PAS 71:2005. BSI. London.

Declaration Exercice. (2024). Access 10.07.2024 from https://www.r-nano.fr/?locale=en

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market. OJ L 178 of 17/07/2000.

Environment Directorate, Chemicals and Biotechnology Committee, Chemical Accidents Involving Nanomaterials: Potential Risks and Review of Prevention, Preparedness and Response Measures – Project Report Series on Chemical Accidents. ENV/CBC/MONO(2022)19, 2022, No. 34. Access 06.07.2024 from https://one.oecd.org/document/env/cbc/mono(2022)19/en/pdf

European Commission, Scientific Committee on Emerging and Newly Identified Health Risks, SCENIHR/002/05. Access 16.07.2024 from https://ec.europa.eu/health/scientific_committees/opinions_layman/en/nanotechnologies/l-3/1-introduction.htm

European Observatory for Nanomaterials (EUON). Access 01.07.2024 from https://euon.echa.europa.eu/pl/about-us

Florek, I.B., Eroglu, S.E. (2019). *The need for protection of human rights in cyberspace.* Journal of Modern Science, Vol. 3/42/2019, p. 27, https://doi.org/10.13166/jms/112765

Janković, N., Plata, D. (2019). *Engineered nanomaterials in the context of global element cycles, Environmental Science*: Nano 6/9, 2697-2711. https://doi.org/10.1039/c9en00322c

Kosieliński, S. (2017). *Rynek dronów w Polsce, edycja 2017, Świat w Dolinie Śmierci.* Fundacja Instytut Mikromakro, partner wydania CNBOP-PIB, Warszawa.

Mrowiec, B. (2016). *Kierunki i możliwości bezpiecznej gospodarki nanoodpadami*. CHEMIK 70, 10, pp. 593–596.

Nanotechnology Regulation and the OECD, CIEL Center for International Environmental Las, CCOS, Oko-Institut. Access 02.07.2024 from https://ecostandard.org/wp-content/uploads/nano-reg-oecd.pdf

Nanoregister. Healt Belgium. Access 10.07.2024 from https://www.health.belgium.be/en/environment/chemical-substances/nanomaterials/register

Ocena ryzyka pożarowego w instalacjach fotowoltaicznych. Określenie koncepcji bezpieczeństwa w celu minimalizacji ryzyka. Wydawnictwo CNBOP-PIB Józefów 2021, ISBN: 978-83-958583-0-7

Project Environmet Directorate, Chemicals and Biotechnology Committee, Chemical Accidents Involving Nanomaterials: Potential Risks and Review of Prevention, Preparedness and Response Measures – Project Report Series on Chemical Accidents. ENV/CBC/MONO (2022), No. 34. Access 02.07.2024 from https://one.oecd.org/document/env/cbc/mono(2022)19/en/pdf

Rabajczyk, A., Wyszomirska, M., Zboina, J. (2024). *Selected aspects of the use of nanotechnology – solutions and challenges in the field of safety and in the regulatory area*. Zeszyty Naukowe SGSP 1 (89): pp. 63-84; DOI: 10.5604/01.3001.0054.4248

Rabajczyk, A., Zielecka, M., Hopke, P., Porowski, R. (2020). *Metal nanoparticles in the air – State of the art and future perspectives*: Environmental Science-Nano 7, DOI: 10.1039/D0EN00536C

Rabajczyk, A., Zielecka, M. (2020). *Emission of metal nanoparticles to the environment as a result of industrial processes*: Przemysł Chemiczny 1(7), pp. 48-51. DOI: 10.15199/62.2020.7.7

Regulation (EC) No 1907/2006 of the European Parliament and of the council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC. OJ L 396 30.12.2006.

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Journal Device UE L 257 of 28/08/2014, p. 73.

Commission Regulation (EU) 2024/858 of 14 March 2024 amending Regulation (EC) No 1223/2009 of the European Parliament and of the Council as regards the use of nanomaterials in cosmetic products: styrene/acrylic copolymer, sodium salt of styrene/acrylic copolymer, copper , colloidal copper, hydroxyapatite, gold, colloidal gold, gold with thioethylamine and hyaluronic acid, acetylheptapeptide-9 with colloidal gold, platinum, colloidal platinum, acetyltetrapeptide-17 with colloidal platinum and colloidal silver. OJ L, 2024/858, 15/03/2024. Access 02.07.2024 from *http://data.europa.eu/eli/reg/2024/858/oj*

Sitek, M. (2023). *Prawo człowieka do środowiska w kontekście nowego pakietu UE fit for 55*, Journal of Modern Science 3/52/2023 p. 18, https://doi.org/10.13166/jms/172891

Such-Pyrgiel, M., Rosińska-Wielec, E. (2024). *Platforma internetu rzeczy jako wsparcie cyfryzacji przedsiębiorstw na przykładzie projektu LINGARO IOT CLOUD PLATFORM,* Journal of Modern Science 1/55/2024 p. 33, https://doi.org/10.13166/jms/185333

The Royal Society 2004. Access 02.07.2024 from https://royalsociety.org/-/media/policy/publications/2004/9693.pdf

Wyszomirska, M. (2023). *Rozwój technologii jako nowe wyzwanie dla współczesnego prawodawstwa,* Wydawnictwo Safty α Fire Technology, DOI: 10.12845/sft.62.2.2023.6, pp.112 – 118.

Wyszomirska, M. (2024). *Prawodawstwo krajowe i unijne wobec wyzwań technologii XXI wieku – wybrane przepisy dotyczące ochrony danych oraz bezpieczeństwa osób i produktów,* Wydawnictwo Safty α Fire Technology, Vol. 63, Issue 1/2024 pp. 96-110.

Wytyczne w zakresie ochrony przeciwpożarowej garaży w obiektach budowlanych, przeznaczonych do ładowania samochodów elektrycznych i hybrydowych plug-in. Wydawnictwo CNBOP-PIB Józefów 2024, ISBN: 978-83-971388-0-3.

Zalecenie Komisji z dnia 10 czerwca 2022 r. dotyczące definicji nanomateriału (2022/C 229/01).

Zboina, J. (2020) *Badania i wdrożenia. Interdyscyplinarność badań bezpieczeństwa,* Wydawnictwo CNBOP Józefów 2020, ISBN 978-83-948534-8-8.