Digitalisation of water services and the water sector cyber threat landscape: Is the EU regulatory framework adequate?

Markopoulou, Dimitra; Papakonstantinou, Vagelis

Published in:
Journal of Water Law

Publication date:
2021

DIGITALISATION OF WATER SERVICES AND THE WATER SECTOR CYBER THREAT LANDSCAPE: IS THE EU REGULATORY FRAMEWORK ADEQUATE?*

DIMITRA MARKOPOULOU and VAGELIS PAPAKONSTANTINOU
Vrije Universiteit Brussel

INTRODUCTION

Critical infrastructures are vital for the functioning of modern societies.[1] Over recent decades the number, variety and complexity of critical infrastructures have increased significantly and so too has their exposure to different types of threats that vary from natural disasters and human errors to theft or even terrorist attacks. However, in the last 20 years a new type of threat has made its appearance in the critical infrastructure landscape, that of cyberattacks. Two different factors make critical infrastructures an attractive target for cyber criminals. The first refers to the nature of critical infrastructures as a vital public good, a realisation that creates an opportunity for large profits for the attacker. The second refers to the constantly increasing application of information and communication technology (ICT) in the operation and management of critical infrastructures, specifically their incorporation into industrial control systems (ICSs).

With regard to the second factor in particular, most critical infrastructures nowadays, such as those pertaining to energy, oil, transportation and water are controlled and monitored by ICSs. ICS is a general term that describes industrial automation systems entrusted with data acquisition, visualisation and control of industrial processes, that are often found in various industrial sectors and critical infrastructures.[2] ENISA notes in a report released in 2015 that 'the ICS-SCADA environment is the fundamental component of European and national critical infrastructures'.[3] However, both the indispensable contribution of ICSs to the operation of critical infrastructures and their vulnerabilities,[4] that are mainly attributable to their open architecture and their increasing connectivity to external information systems, have made ICSs a priority target for cyber criminals.[5]

Exposure of critical infrastructures to cyber risks due to their high dependence on ICSs has been further intensified over the last years by the extensive use and installation of smart devices (smart meters and sensors) to consumers' homes. Through them operators of critical infrastructures are afforded not only remote control and monitoring of the operation of their infrastructures and networks but also direct access to consumers' homes. The massive collection of personal information performed by these devices as well as their vulnerabilities are an additional concern for regulators and critical services providers.

The drinking water and water transportation sector is unquestionably categorised as a critical infrastructure.[6] The Organisation for Economic Cooperation and Development (OECD), in its Environmental Outlook to 2030, states that water demand is expected to rise globally by 55 per cent between 2000 and 2050; by 2050, up to 3.9 billion people, 40 per cent of the world's population, may be living in water-stressed areas.[7] The statistics on water scarcity together with climate change have motivated governments and water utilities/suppliers to develop and implement innovative techniques in order to warrant efficient water management solutions. In this context, terms such as 'smart water', 'smart water management', 'smart water networks' and 'smart water grids and meters' are currently used by the water sector in order to describe the integration of ICT into the water infrastructures or, in short, water digitalisation.

Within a water digitalisation context, the water sector has followed the example of other sectors, most notably energy, in increasing its dependence on ICT for improving its service, sustainability and affordability. Even though the integration of ICT has not yet reached the maturity level of the energy sector, an ever-increasing number of

* This article was written in the context of an H2020 research project (NAIADES).

1 On the definition of critical infrastructures see Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Article 2(a) defines critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.

2 ICSs include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and programmable logic controllers (PLC). SCADA systems are highly distributed systems used to control geographically dispersed assets, where centralised data acquisition and control are critical to system operation. In the water sector, they are used in water distribution and wastewater collection systems. A DCS is a control architecture that supervises multiple, integrated sub-systems responsible for controlling the details of a localised process, such as water and wastewater treatment. PLCs are computer-based solid-state devices that control industrial equipment and processes.

3 ENISA 'Analysis of ICS-SCADA cyber security maturity levels in critical sectors' (2015).

4 For vulnerabilities of ICSs see Cristina Alcare and Sherali Zeadally 'Critical infrastructure protection: requirements and challenges for the 21st century' (2015) 8 *International Journal for Critical Infrastructure Protection* 53.

5 On the definition and protection of ICSs see J Weiss 'Industrial control system (ICS) cyber security for water and wastewater systems' in Robert M Clark, Simon Hakin *Securing Water and Wastewater Systems* (Springer International Publishing 2014).

6 ENISA (n 3).

7 See C S Laspidou 'ICT and stakeholder participation for improved urban water management in the cities of the future' (2014) 8 *Water Utility Journal* 79 https://www.ewra.net/wuj/pdf/WUJ_2014_08_08.pdf.

water suppliers and operators of water utilities depend on ICT to operate and monitor processes remotely such as testing the quality of water, monitoring the pressures and flows in water and wastewater pipelines, controlling the treatment processes and managing its distribution. The use of smart devices, such as sensors and meters, has improved the ability to monitor in real time and control water distribution, to prevent and respond to harms in the water network (for instance to detect pollutants or water infection before water reaches consumers), to detect leakages and bursts, to measure the consumption of water and improve its management and to lower losses, as well as to regulate water flow inside the distribution system.[8]

While ICT may increase the water sector's productivity and reliability, at the same time it makes it increasingly vulnerable to malicious cyberattacks or accidental cyber incidents. In practice, the ongoing implementation of ICS on water networks has broadened the attack surface within water companies. It is true that attacks against critical infrastructures have increased over recent years with the water domain being no exception to this rule.[9] The consequences of a possible interruption or compromise of the water sector's ICS, for example manipulation or disruption of water services, damage to equipment or compromise of water safety, could prove disastrous both for public health and safety and due to economic loss. At the same time, water sector entities are responsible for processing and accordingly protecting personal information, including employees' records and customers' billing data. This personal information is an attractive target for cybercriminals. Installation of smart devices in consumers' homes, that is expected to increase in the years to come following the example of the energy sector, makes any discussions regarding the protection of consumers' personal data against unauthorised access and use even more relevant.

The constantly increasing number of cyberattacks against critical infrastructures has turned their protection, as well as the protection of the network and information systems that support them, into a high priority for the EU. Safeguarding their integrity, confidentiality and availability has been high on the EU agenda over decades. Its efforts have led to the introduction of a detailed EU regulatory framework that addresses both cybersecurity concerns, as well as issues related to the protection of personal data. With regard to the water sector in particular, safeguarding the continuity and integrity of water services and ensuring a satisfactory level of water quality has been intensively discussed among EU regulatory bodies since the mid-1970s. Nevertheless, the current EU regulatory framework does not deal with the protection of water facilities against cyber risks. Rather, security within the water domain is perceived only within the sense of safe water supply and sanitation, adequate protection from water-related disasters and diseases, as well as acceptable cost, quality and quantity of water. However, following digitalisation, the water industry needs to secure its systems further as part of the ICT landscape.

This article will examine the effect of the EU regulatory framework on water management from both a sector-specific and a cybersecurity perspective. The next section examines the current water management regulatory framework, placing emphasis on its main legislative instrument, the Water Framework Directive. Next, EU cybersecurity policy is analysed in the context of the regulatory regime on the security of network and information systems and on the protection of critical infrastructures. The NIS Directive and the Directive on the Protection of European critical infrastructures will be specifically addressed in this section. In the following section, the focus is on the applicability of the General Data Protection Regulation on the water sector, with particular attention paid to concerns caused by smart water management and the use of smart devices in consumers' homes. Lastly, the final section evaluates the adequacy and efficiency of the relevant regulatory instruments for the protection of water facilities and water services against cyber incidents within the new digitalised water landscape, identifying a need for a shift in approach in order to create a more cyber resilient water sector.

THE EU REGULATORY FRAMEWORK APPLICABLE TO WATER SERVICES, WATER RESOURCE MANAGEMENT AND ENVIRONMENTAL MONITORING

European water policy on the protection of water and the promotion of a sustainable approach to water management has been through a complex and lengthy development period, which has eventually led to the current regulatory framework. Specifically, early European water legislation, also referred to as the first wave of water legislation, began in 1975 with the introduction of standards for rivers and lakes that were used for drinking water abstraction. The adoption in 1991 of the Urban Waste Water Treatment Directive[10] and the Nitrates

8 On the definition of smart water management and smart water system technologies see also H M Ramos and others 'Smart water management towards future sustainable networks' (2020) 12 *Water* 58 (Special Issue 'New challenges on water systems' https://doi.org/10.3390/w12010058).

9 One of the most notorious cyberattacks in the water sector includes the Maroochy Shire attack, which was carried out on Maroochy Shire Council's sewage control system in Queensland, Australia, threatening public health and safety. The offences occurred between 9 February 2000 and 23 April 2000. Vitek Boden accessed computers controlling Maroochy Shire Council's sewerage system, altering electronic data (in particular sewerage pumping stations) and causing malfunctions in their operations. As a result, pumps did not run when needed and alarms were not reported. Sewage flooded a nearby park and contaminated an open surface-water drainage ditch and flowed into a tidal canal. See also https://www.csoonline.com/article/3541837/attempted-cyberattack-highlights-vulnerability-of-global-water-infrastructure.html. In April 2020, Israel's National Cyber Directorate received reports about an attempted 'major' cyberattack on its water infrastructure. According to a statement issued by the directorate, the attack consisted of assault attempts on control and control systems of wastewater treatment plants, pumping stations and sewers. The attempted attacks were unsuccessful. In July 2020, two more cyberattacks hit Israel's water management facilities. The attacks did not cause any damage to the attacked organisations. The first attack hit agricultural water pumps in upper Galilee, while the second one hit water pumps in the central province of Mateh Yehuda. Highly placed sources from the water authority of Israel stated that the hackers tried to modify the chlorine induction levels facilitated into the reservoirs. See also https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/. On cyberattacks on the US water infrastructures see J H Germano 'Cybersecurity risk and responsibility in the water sector' (American Water Works Association 2019) https://www.awwa.org/Portals/0/AWWA/Government/AWWACybersecurityRiskandResponsibility.pdf. See also 'Water infrastructure: when states and cyberattacks rear their ugly heads' https://www.stormshield.com/news/water-infrastructure-when-states-and-cyber-attacks-rear-their-ugly-heads/.

10 See Council Directive 91/271/EEC of 21 May 1991 concerning urban wastewater treatment.

Directive[11] marked the beginning of the second wave of water legislation. In 1995, following requests from the European Parliament's Environmental Committee and the Council of the Environment Ministers, the Commission considered the need for a holistic approach to water policy and in particular the need for a single piece of legislation to tackle these issues. The outcome of this process was the Water Framework Directive,[12] which introduced a single system of water management, namely river basin management.[13]

The WFD entered into force on 22 December 2000. It is one of the leading documents regulating EU water policy and its main objective is to expand the scope of water protection to all waters, surface waters and groundwater, as well as to achieve a good status for all EU waters including fresh, transitional (river mouths) and coastal waters. To do so it takes a pioneering approach to protecting water that is based not on administrative or political boundaries but on natural geographical formations: river basins. River basin planning is a term used to refer to the management of land and water as a system.[14] The WFD therefore offers an integrated and coordinated approach to water management in Europe based on exactly this concept. It is complemented by a number of other regulations governing specific aspects of water policy including urban wastewater, nitrates, industrial emissions, pesticides, bathing and drinking water.

With regard to specific regulatory instruments that complement the WFD, the Groundwater Directive[15] was introduced in response to requirements of Article 17 of the WFD, which set the framework for preventing and controlling the pollution of groundwater.[16] The directive was adopted in December 2006 and it establishes a regime that sets groundwater quality standards and introduces measures to prevent or limit inputs of pollutants into groundwater.[17] In this context it outlines chemical status criteria that the Member States need to follow to monitor and assess groundwater quality on the basis of common criteria, as well as the measures they need to adopt in order to prevent or limit inputs of pollutants into groundwater.

The second piece of legislation that complements the WFD is the Directive on Environmental Quality Standards.[18] The directive's legal basis is found in Article 16(1) of the WFD, according to which Member States must implement the necessary measures with the aim of progressively reducing pollution from priority substances. The list of these substances is, according to the directive, proposed by the Commission and, upon adoption by the Council and the Parliament, becomes an Annex to the WFD (Annex X). The first list of priority substances was established by way of Decision 2455/2001/EC and it was later replaced by Annex II of the Priority Substances Directive.[19] The directive specifies 35 substances or groups of substances for which environmental quality standards were set in 2008. The list of priority substances and the EQSD were amended again by Directive 2013/39/EU[20] which resulted in identification of ten additional priority substances (45 in total).[21]

Other legislative instruments that complement the EU water policy include the Urban Wastewater Treatment Directive and the Nitrates Directive, which together tackle the problem of eutrophication (as well as health effects such as microbial pollution in bathing water areas and nitrates in drinking water). The Urban Wastewater Directive[22] was adopted on 21 May 1991. Its objective is to protect the environment from the adverse effects of urban wastewater discharges and from certain industrial discharges.[23] The Nitrates Directive[24] is one of the key instruments in the protection of waters against agricultural pressures. It was adopted on 12 December 1991. The directive aims to protect water quality across Europe by preventing nitrates from agricultural sources polluting ground and surface waters and by promoting the use of good farming practices.

The Water Framework Directive is also closely linked to the Marine Directive. Its goal of achieving 'good status' for all EU surface and groundwaters is tied in with the goal of good environmental status (GES) of the EU's marine waters under the Marine Directive. The Marine

11 See Council Directive of 12 December 1991 concerning the protection of waters against pollution caused by nitrates from agricultural sources (91/676/EEC).

12 See Directive 2000/60/EC of the European Parliament and of the Council establishing a framework for the Community action in the field of water policy.

13 On the description of the directives and their background see also the Commission's Staff Working Document 'Fitness check of the Water Framework Directive, Groundwater Directive, Environmental Quality Standards Directive and the Floods Directive' (2019) SWD 439 final, ch 2.

14 On the WFD see also N Voulvoulis, K D Arpon and T Giakoumis 'The EU Water Framework Directive: from great expectations to problems with implementation' (2016) 575 *Science of the Total Environment* 358 https://www.researchgate.net/publication/309202900_The_EU_Water_Framework_Directive_From_great_expectations_to_problems_with_implementation.

15 See Directive 2006/118/EC of 12 December 2006 on the protection of groundwater against pollution and deterioration [2006] OJ L372 (27 December 2006).

16 Article 17(1) of the Groundwater Directive reads as follows: 'Strategies to prevent and control pollution of groundwater 1. The European Parliament and the Council shall adopt specific measures to prevent and control groundwater pollution. Such measures shall be aimed at achieving the objective of good groundwater chemical status in accordance with Article 4(1)(b) and shall be adopted, acting on the proposal presented within two years after the entry into force of this Directive, by the Commission in accordance with the procedures laid down in the Treaty'.

17 The directive constitutes a continuation of Directive 80/68/EEC on the protection of groundwater against pollution caused by dangerous substances, which was repealed in 2013.

18 See Directive 2008/105/EC of 16 December 2008 on environmental quality standards in the field of water policy, amending and subsequently repealing Council Directives 82/176/EEC, 83/513/EEC, 84/156/EEC, 84/491/EEC and 86/280/EEC and amending Directive 2000/60/EC of the European Parliament and of the Council.

19 The list of priority substances (Annex X to the WFD), and the EQSD were amended by Directive 2013/39/EU (Directive 2013/39/EU of the European Parliament and of the Council of 12 August 2013 amending Directives 2000/60/EC and 2008/105/EC as regards priority substances in the field of water policy Text with EEA relevance), which resulted in 10 additional priority substances being added to the list, making 45 in total.

20 See Directive 2013/39/EU of 12 August 2013 amending Directives 2000/60/EC and 2008/105/EC as regards priority substances in the field of water policy (Text with EEA relevance) [2013] OJ L226 (24 August 2013) 1–17.

21 Directive 2013/39/EU introduced a mechanism to obtain monitoring data to inform the Commission's reviews of the priority substances list, The watch list was established in 2015; it was updated in 2018, and again in 2020. Member States have to monitor the substances on the list at least once each year for up to four years.

22 See n 10.

23 See n 21.

24 See n 11.

Strategy Framework Directive was adopted on 17 June 2008.[25] It is the first EU legislative instrument related to the protection of marine biodiversity, and it contains the explicit regulatory objective that 'biodiversity is maintained by 2020' as the cornerstone for achieving GES. The Commission adopted a report on the first implementation cycle of the Marine Strategy Framework Directive in June 2020. This report (as required by Article 20 of the directive) shows that while the EU's framework for marine environmental protection is one of the most comprehensive and ambitious worldwide, it needs to be strengthened to be able to tackle predominant pressures such as overfishing and unsustainable fishing practices, plastic litter, excess nutrients, underwater noise and others types of pollution.

Finally, the Drinking Water Directive[26] concerns the quality of water intended for human consumption. Its objective is to protect human health from adverse effects of any contamination of water intended for human consumption by ensuring that it is wholesome and clean. On 16 December 2020, the European Parliament formally adopted the revised Drinking Water Directive.[27] The directive entered into force on 12 January 2021, and Member States will have two years to transpose it into national legislation.[28]

It is undoubtedly true that protection of water resources is one of the cornerstones of environmental policy in Europe. However, despite the significant initiatives that have been undertaken at European level and the progress achieved so far, the framework on water protection and on sustainable water management does not take into consideration the cyber security risks that threaten water supply infrastructures. As already mentioned above, security issues in the context of the WFD are only perceived as risks that concern the quality and the abundance of water. Consequently, no cyber security-related concerns or incident management requirements are to be found within current EU water legislation. On the contrary, as will be seen in the analysis that follows, they are to be found incidentally in other legislation that places water management, among other public facilities, within its scope.

THE APPLICABILITY OF THE EU CYBERSECURITY STRATEGY ON THE WATER SECTOR: THE EU CYBERSECURITY REGULATORY FRAMEWORK AND THE PROTECTION OF CRITICAL INFRASTRUCTURES

The EU cybersecurity regulatory framework: The NIS Directive and the role of ENISA in protecting critical infrastructures against cyber threats

The EU has been addressing cybersecurity issues in a comprehensive manner since 2004, when ENISA (the European Union Agency for Network and Information Security) was founded. The cornerstone of the European policy on cybersecurity, the NIS Directive,[29] entered into force in August 2016; however, it has its roots in the Communication released by the Commission in 2009 on critical information infrastructure protection from large-scale cyberattacks.[30] Initial thoughts on the adoption of a legislative framework for the protection of network and information systems against cyber risks became more concrete in the cybersecurity strategy of the EU, which was released in 2013.[31] The vital role that network and information systems play in the society and the need to protect their reliability and security against cyber incidents was specifically identified in this document. The directive eventually entered into force in August 2016 following two years of intensive discussions between the Commission, the Council and the Parliament. The NIS Directive is the first horizontal legislation undertaken at EU level for the protection of network and information systems across the Union.[32]

The NIS Directive does not make any explicit reference to critical infrastructures; however, it uses the term operators of essential services which should be considered equivalent. According to the definition introduced by the directive, operators of essential services include all public or private entities that provide a service which is essential for the maintenance of critical societal and/or economic activities. The specific sectors that fall under the category of OES are listed in Annex II of the directive and include the following sectors; energy, transport, banking, financial market infrastructures, health, drinking water supply and distribution and digital infrastructure. The NIS Directive adopts a further step in identifying operators of essential services: once an entity is categorised as one of the types listed in the Annex, the next step lies with the Member States, who are responsible for carrying out an identification process in order to determine which individual companies meet the additional criteria of the definition of operators of essential services.[33] To this end, the NIS Directive requires Member States to adopt national measures as a result of the identification process, in order to determine these entities.[34] Eventually, all

25 See Directive 2008/56/EC establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive).

26 See Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption.

27 See Directive EU 2020/2184 of 16 December 2020 on the quality of water intended for human consumption.

28 On the key features of the revised directive see also https://ec.europa.eu/environment/water/water-drink/review_en.html.

29 See 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.

30 See Communication from the Commission on critical information infrastructure protection 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience' COM/2009/0149 final.

31 See Joint Communication on the cybersecurity strategy of the European Union 'An open, safe and secure cyberspace' JOIN/2013/01 final.

32 See also Dimitra Markopoulou, Vagelis Papakonstantinou and Paul de Hert 'The new EU cybersecurity framework: the NIS Directive, ENISA's role and the General Data Protection Regulation' (2019) 35(6) *Computer Law and Security Review* 1.

33 See art 5 of the NIS Directive on identification of operators of essential services.

34 See also recital 25 of the NIS Directive, which reads as follows: 'as a result of the identification process, Member States should adopt national measures to determine which entities are subject to obligations regarding the security of network and information systems. This result could be achieved by adopting a list enumerating all operators of essential services or by adopting national measures including objective quantifiable criteria, such as the output of the operator or the number of users, which makes it possible to determine which entities are subject to obligations regarding the security of network and information systems. The national measures, whether already existing or adopted in the context of this Directive, should include all legal measures, administrative measures and policies allowing for the identification of operators of essential services under this Directive'.

entities that are identified as operators of essential services by the Member State within which they are established, need to comply with the security and notification requirements that the NIS Directive provides for their respective category.

With regard to the water sector in particular, water management is a notion frequently found in the NIS Directive text.[35] The NIS Directive approaches water in a twofold manner: that is, within the context of transport and within the context of drinking water. Both are placed under the definition of operator of essential services of Article 4(4), which states that 'for the purposes of this Directive the following definitions apply: (4) "operator of essential services" means a public or private entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2)'. Accordingly, under its Annex II, 2(c) refers to water transport and 6 refers to drinking water supply and distribution.[36] Therefore, inland, sea and coastal passenger and freight water transport companies and suppliers and distributors of water intended for human consumption fall under the NIS Directive's definition of operators of essential services. As a result, once the identification process of Article 5 of the Directive is completed, all identified entities of the water transport and the drinking water sectors must comply with the security and notification requirements described in its text as regards protection of their network and information systems.

Security requirements are regulated under Article 14(1) and Article 14(2) of the NIS Directive. Article 14(1) sets the Member States' obligation to ensure that operators of essential services take appropriate measures, technical and organisational, to manage the risks posed to the security of the network and information systems they use. In accordance with Article 14(2), appropriate measures shall prevent and minimise the impact of incidents affecting the security of their systems. Security requirements are further defined in the reference document on security measures for OES developed by the Cooperation Group.[37]

Notification requirements are regulated under Article 14(3), according to which Member States have to ensure that operators of essential services notify 'any incident having a significant impact on the continuity of the essential services'. A definition regarding the continuity of service is missing from the NIS Directive, but it is our understanding that in this particular context, where the essential services are critical for societal and/or economic activities, continuity should be understood as the provision of a service at an agreed/reasonable standard of quality. For example, in the case of the drinking water subsector, the lack of water due to cyber issues would certainly constitute a cyber incident; however, the same would most likely also be the case with improper provision of water (due to cyber issues) in terms of quantity, quality or other relevant parameters. Continuity does not mean only availability but also the proper provision of the essential service, a term that is usually assimilated in practice with business continuity.

In this context, operators of essential services are not mandated to notify any minor incidents but only serious ones, affecting the continuity of their essential service. Article 14.4 provides a list of factors that should be taken into account when determining the significance of the impact of an incident, namely the number of users affected, the duration of the incident and the geographical spread with regard to the area affected by the incident. Again, consistency in the national approaches, as far as the notification process is concerned, is of the essence. As in the case of security requirements, the Cooperation Group has published a reference document on this issue.[38]

The NIS Directive finds full applicability in the drinking water sector. Water network operators and water suppliers need to apply its provisions in order to safeguard the protection of their networks against cyber threats. The NIS Directive and accompanying guidance by the Cooperation Group provide significant assistance to all water entities that fall under the definition of an operator of essential services to implement the necessary requirements and make their organisations more cyber resilient. Recently, the EU adopted a proposal on a new directive on measures for a common level of cybersecurity across the Union.[39] A thorough analysis of the proposal is beyond the scope of this article. What is worth mentioning, however, is that the proposal abandons the notion of operator of essential services, which is substituted by the terms 'essential entity' and 'important entity'. The list of sectors that fall within the scope of the directive is widened to include the wastewater sector, public administration and space. As will be elaborated below in the section on critical infrastructures protection, the Annex is updated to align with the respective Annex of the new proposal on the European Critical Infrastructures (ECI) Directive. Consequently, once the new directive enters into force, all entities that fall within the water supply and the wastewater sectors and fulfil the criteria of an essential entity will need to implement the security and notification requirements indicated by that directive's provisions.

ENISA, for its part, has developed a series of guidelines in order to assist Member States to implement the NIS Directive, including a tool that maps security measures for operators of essential services to international

35 See recital 10: 'In the water transport sector, security requirements for companies, ships, port facilities, ports and vessel traffic services under Union legal acts cover all operations, including radio and telecommunication systems, computer systems and networks. Part of the mandatory procedures to be followed includes the reporting of all incidents and should therefore be considered as lex specialis, in so far as those requirements are at least equivalent to the corresponding provisions of this Directive' and recital 11 'When identifying operators in the water transport sector, Member States should take into account existing and future international codes and guidelines developed in particular by the International Maritime Organisation, with a view to providing individual maritime operators with a coherent approach'.

36 Suppliers and distributors of water intended for human consumption as defined in art 2(1)(a) of Council Directive 98/83/EC but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services.

37 See the Cooperation Group's reference document on security measures for operators of essential services, https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

38 See Reference document on incident notification for operators of essential services. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

39 See Proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM/2020/823 final.

standards,[40] as well as, a report on mapping of operators of essential services' security requirements to specific sectors.[41] ENISA's role in supporting the NIS Directive's implementation and in contributing to increasing cybersecurity capabilities at Union level is further strengthened by the Cybersecurity Act.[42] Among the objectives of the new regulation, which came into force on 27 June 2019, is the strengthening of ENISA's role by granting to it a permanent mandate and the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes.

In addition to its contribution to the implementation of the NIS Directive, ENISA has also identified the extended use of ICS in the process of monitoring and controlling the functioning of critical infrastructures, as well as the high cyber risks that these systems cause. At the same time, it has recognised the significant impact cyberattacks may have on critical infrastructures and services. In this context, it has published several reports on the identification of critical infrastructures and their protection.[43,44] Recently, ENISA issued guidelines on cyber risk management for ports,[45] railway cybersecurity[46] and cybersecurity for hospitals,[47] thus targeting the maritime, transport and health sectors, respectively. In addition to these initiatives, ENISA has specifically addressed the sectors of health, finance, maritime and railway in the context of its approach on critical infrastructures and services. However, it seems that the water sector has not yet attracted ENISA's targeted attention. This could be partially attributed to the fact that, as depicted in the findings of a survey of 251 organisations across five EU Member States with regard to NIS investments four years after the directive entered into force, drinking water distribution is among the sectors least affected by major information security incidents, while the sectors most affected are the banking and healthcare sectors.[48] As the digitalisation of water services progresses and the cyber risks become more frequent and severe, it is anticipated that ENISA will soon respond to new challenges and provide the necessary guidance and assistance in making the water sector more cyber resilient.

The European programme for critical infrastructure protection: the 2008 Directive on European critical infrastructures

The EU has been engaged in supporting the protection of critical infrastructures since 2004 when the Commission published its Communication on Critical Infrastructure Protection in the fight against terrorism.[49] The document made an official introduction to the notion of critical infrastructures defining them as, 'critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy, including banking and finance, transport and distribution, energy, utilities, health, food supply and communications, as well as key government services'. Several initiatives followed, including a Green Paper that was adopted by the Commission in November 2005.[50] The main purpose of the Green Paper was to receive feedback concerning a possible European programme on critical infrastructure protection policy options by involving a broad number of stakeholders. Eventually, the European programme for critical infrastructure protection (EPCIP) was presented by the Commission in 2006.[51] In 2009, the Commission adopted a Communication on critical information infrastructure protection setting out a plan (the CIIP Action Plan) to strengthen the security and resilience of vital ICT infrastructures.[52] In 2011, a new Communication was released by the Commission, which focused on the evaluation of the achievements and next steps of the CIIP action plan.[53] A new approach on the EPCIP plan was incorporated in the Commission's Staff Working Document, which was adopted in 2013 to take account of increasing cross-border interdependencies.[54,55]

The main legislative instrument of the Commission's EPCIP is the 2008 Directive on European critical infrastructures.[56] The directive defines European critical infrastructure as 'an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions'.[57] However, despite its innovative character,

40 See ENISA's tools on security measures for OES https://www.enisa.europa.eu/news/enisa-news/enisa-launches-oes-tool-to-map-security-measures.

41 See ENISA's report on mapping of OES security requirements to specific sectors (January 2018) https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.

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

43 See ENISA's report on Stocktaking, Analysis and Recommendations on the protection of CIIs, January 2016.

44 See ENISA's report on methodologies for the identification of Critical Information Infrastructure assets and services (February 2015).

45 See ENISA's guidelines on Cyber Risk Management for Ports (December 2020).

46 See ENISA's report on Railway Cybersecurity (November 2020).

47 See ENISA's report 'Procurement guidelines for cybersecurity in hospitals' (February 2020).

48 See ENISA's NIS Investment Report (December 2020) https://www.enisa.europa.eu/publications/nis-investments.

49 See Communication from the Commission on Critical Infrastructure Protection in the fight against terrorism, COM/2004/0702 final.

50 See Green Paper on a European programme for critical infrastructure protection, COM/2005/0576 final.

51 See Communication from the Commission of 12 December 2006 on a European programme for critical infrastructure protection, COM(2006) 786 final.

52 See Commission's Communication on critical information infrastructure protection – 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM(2009) 149 final.

53 See Commission's Communication on critical information infrastructure protection – 'Achievements and next steps: towards global cybersecurity', COM(2011) 163.

54 See Commission's Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection – 'Making European critical infrastructures more secure', SWD/2013, 318.

55 See also Dimitra Markopoulou and Vagelis Papakonstantinou 'The regulatory framework for the protection of critical infrastructures against cyber threats: identifying shortcomings and addressing future challenges: the case of the health sector in particular' (2021) 41 *Computer Law and Security Review* 1.

56 On the regime of European critical infrastructures see also V Coroiu 'European critical infrastructures' (2015) 6(2) *European Journal of Public and National Security* 1.

57 On the definition of critical infrastructures see also Kristian Cedervall Lauta 'Regulating a moving nerve: on legally defining critical infrastructure (2015) 6(2) *European Journal of Risk Regulation* 176.

the directive adopts a sector-specific approach, limiting its implementation to the energy and transport sectors only. Several policy sectors, such as the health sector or the drinking water supply and distribution sector or the financial sector are therefore left outside its scope. This limitation is acknowledged in its text, where it is specifically mentioned that, by the time of its review, subsequent sectors may be identified, with a priority to be given to the ICT sector.[58] Furthermore, its implementation by the Member States has been questioned because, to date, only 94 ECIs have been designated, two-thirds of which are located in three Member States in Central and Eastern Europe. In view of these concerns, during 2018–19 the directive was the subject of an external evaluation. The evaluation was finalised on 23 July 2019 through the publication of a Staff Working Document.[59]

In July 2020, the Commission adopted the EU Security Union Strategy,[60] which, among others, identified the increasing interconnection and interdependency between physical and digital infrastructures. On this basis, it underlined the need for a more coherent and consistent approach between the ECI Directive and the NIS Directive. In view of the remarks, on December 2020 the Commission presented a Proposal for a Directive on the resilience of critical entities.[61] This proposal reflects the priorities of the Commission's EU Security Union Strategy, which calls for 'a revised approach to critical infrastructures resilience that better reflects the current and anticipated future risk landscape, the increasingly tight interdependencies between different sectors, and also the increasingly interdependent relationships between physical and digital infrastructures'. The proposed directive would have a much wider scope covering 10 sectors including energy, transport, banking, financial market infrastructure, heath, drinking water, wastewater digital infrastructure, public administration and space. Furthermore, the proposal is closely aligned with the proposal on a new NIS Directive and aims to ensure that 'the competent authorities under both legal acts take complementary measures and exchange information as necessary regarding cyber and non-cyber resilience and that particularly critical operators in the sectors considered to be essential per the proposal at hand are also subject to more general resilience enhancing obligations'.[62]

As regards the water sector in particular, it is identified as a critical infrastructure in all EU documents concerning the EU policy on their protection. Although it is not specifically addressed by the ECI Directive, which, as already mentioned, has been identified as an omission and a gap in the existing legislation, the Commission's new proposal aims not only to include the drinking water sector in its respective Annex but also to expand its applicability in the wastewater sector.

58 See art 3(3) of the 2008 Directive.

59 See Commission Staff Working Document 'Evaluation of Council Directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection', SWD(2019) 310 final.

60 See Communication from the Commission on the EU Security Union Strategy, COM/2020/605 final.

61 See Proposal for a Directive on the resilience of critical entities, COM/2020/829 final.

62 See the explanatory memorandum on the Proposal for a Directive on measures for a high common level of cybersecurity across the Union, COM/2020/823 final.

APPLICABILITY OF THE EU GENERAL DATA PROTECTION REGULATION IN THE WATER SECTOR: SMART DEVICES FOR THE PROVISION OF WATER SERVICES

Water suppliers and network operators as controllers under the GDPR

Water supply and wastewater utilities, both private and public, collect and process personal data of their users for the purpose of providing and billing their services. These include in principle consumers' registration data (names, addresses), usage data (household water consumption), billing data and consumers' payment methods. As regards these data, they fall under Article 4(1) of the GDPR and therefore its provisions are applicable in the water sector.

While the above case is straightforward and does not exceed the boundaries of usual personal data processing for provision of a service, complications may emerge in the context of smart water services or water digitilisation. Should that become the case, depending on the business model applied, complications may appear as early as regarding the controller-processor designation. According to the GDPR the controller 'determines the purposes and means of the processing' while the processor 'processes personal data on behalf of the controller'.[63] In the event, therefore, that water suppliers use third parties for the provision of smart water services, clear delineation between the two as regards the processing of the personal data needs to take place beforehand. Similarly, if water supply was to be separated from water network operation, perhaps along the lines of energy or electronic communications in the EU, the roles of the entities involved for the processing of personal data would have to be clearly defined.

Within the same context of smart water services the categorisation of personal data processed may be significantly affected. Personal data processed under current typical water supply circumstances constitute common data in the GDPR sense, meaning data not falling under the 'special categories' of its Article 9. However, if better quality data were somehow collected from each household's water consumption, for example through examination of wastewater (as has become the case in combating the current Covid-19 pandemic), then such data would presumably be 'identifiable' for the data subjects concerned, in the meaning of Article 4(1) of the GDPR. Health or other data falling under Article 9 of the GDPR could then be inferred from water consumption, a change that would exponentially increase the GDPR compliance requirements for all stakeholders involved.

Risks associated with the use of smart devices for the provision of water services

In addition to the above general obligation of compliance with the GDPR, smart water management services bring additional concerns in terms of safeguarding the security of the consumer's personal data against security data breaches. Smart devices, smart meters and sensors can make water management more efficient and safer for consumers through real-time data collection. However, the real-time collection of consumers' data through these

63 See art 4(7) and 4(8) of the GDPR, respectively.

devices may have an adverse effect on personal data and privacy. Specifically, in order for water suppliers to provide more accurate and customer-oriented services, smart devices collect and sample consumption data from the meters that are installed at consumers' homes regularly, if not daily. At the same time additional information may be stored in the smart meters, such as lot size, irrigable area, number of bathrooms, household population, the presence of swimming pools and irrigation systems to establish individual water budgets and rates based on these budgets.[64] As seen above, under specific circumstances, these data could culminate in 'special categories' of personal data processing within the meaning of Article 9 of the GDPR.

An extensive analysis of the implications of smart devices for the protection of personal data lies beyond the scope of this analysis. However, reference to the main issues their extensive use may involve is considered essential in order to stress the need for the introduction by water network operators or suppliers of adequate safeguards to guarantee the protection of consumers' personal data. As the number of the installed smart water devices grows, the measures that have already been adopted at the EU level to address concerns relating to the use of smart devices by the energy sector are considered relevant for the water sector as well. Under this assumption, and taking into account all particularities of each sector, references to smart grids and meters in the context of the energy sector, shall be applied to smart water devices as well, and any concerns regarding their security against cyber risks as well as regarding the protection of the personal data they process shall be examined, by analogy, from the smart water perspective.

The EU has identified the high risk that the use of smart technologies for the provision of critical services may bring to processing of personal data. As pointed out in the Article 29 Data Protection Working Party opinion:

> [s]mart meters allow for the generation, transmission and analysis of data relating to consumers, much more than is possible with a 'traditional' or 'dumb' meter. Consequently, they also allow the network operator (also known as Distribution Service Operator or DSO), energy suppliers and other parties to compile detailed information about energy consumption and patterns of use as well as make decisions about individual consumers based on usage profiles. Whilst it is acknowledged that such decisions can often be to the benefit of consumers in terms of energy savings, it is also emerging that there is potential for intrusion into the private lives of citizens through the use of devices which are installed in homes'.[65]

In the same context, the European Data Protection Supervisor (EDPS) remarked that:

> [t]he Europe-wide rollout of 'smart metering systems' enables massive collection of personal information from European households, thus far unprecedented in the energy sector. The potential intrusiveness of collection is increased by the fact that data are collected, which may infer information about domestic activities: data may track what members of a household do within the privacy of their own homes'.[66]

Therefore, the use of smart metering and access to information about real-time energy and, by analogy, water consumption may lead to tracking the everyday lives of consumers and accordingly building their profiles based on their domestic activities. Monitoring consumption may help those who have access to these data to draw conclusions about the habits and the behaviours of the consumers, as well as details on the household and its members, such as the holiday periods of the residents, the use of household appliances and the number of residents. Other concerns relate to the use of these data and the consumers' profiles by third parties for marketing and advertising purposes.[67] As commented by the EDPS, law enforcement agencies, tax authorities, insurance companies, landlords, employers and other third parties may also be interested in accessing personal consumption information.[68] In addition to issues of substantive EU personal data protection law, the risks with regard to data security are considerable. Owing to the high value of detailed metering data and of consumers' personal information, cyberattacks are expected to increase in both frequency and intensity. As these devices fall into the category of the Internet of Things (IoT), their inherent vulnerabilities make the risk of cyber incidents even higher.

In view of these challenges and risks, the EU has taken a series of measures to uphold data protection rules, admittedly targeting the energy sector exclusively. This was a reasonable policy option because, at first, smart grids and smart meters were solely deployed by energy network operators and suppliers. Specifically, as early as 2012, the Commission published a Recommendation on preparations for the roll-out of smart metering systems.[69] The Recommendation pointed out that 'One of the key tasks and preconditions for using smart metering systems is to find appropriate technical and legal solutions which safeguard protection of personal data'. The Recommendation suggests certain measures in this direction such as conducting a data protection impact assessment (DPIA) through the use of a DPIA template developed by the Commission. Furthermore, the Recommendation listed specific data protection measures such as anonymising the data, safeguarding the processing of personal data by or within a smart metering system or determining the roles and responsibilities of data controllers and data processors. Finally, with regard to data security, it recommended the use of encrypted channels, smart grids' compliance with security-relevant standards developed by European standardisation organisations and the adoption by network operators of the appropriate security measures to guarantee an adequate level of security and resilience of the smart metering systems.

64 See also Elad Salomons, Lina Sela and Mashor Housh 'Hedging for privacy in smart water meters' (2020) 56(9) *Water Resources Research* 1 https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2020WR027917.

65 See art 29 Working Party Opinion 12/2011 on smart metering https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp183_en.pdf.

66 See the EDPS's Opinion on the Commission Recommendation on preparations for the roll-out of smart metering systems, https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf.

67 On the implications of smart metering for personal data protection see also Rainer Knyrim and Gerald Trieb 'Smart metering under EU data protection law' (2011) 1(2) *International Data Privacy Law* 121.

68 See Lilian Edwards 'Privacy, security and data protection in smart cities: a critical EU law perspective' (2016) 1 *European Data Protection Law Review* 28.

69 See Commission Recommendation 2012/148/EU of 9 March 2012 on preparations for the roll-out of smart metering systems [2012] OJ L73 (13 March 2012).

The Recommendation was followed by an Opinion by the EDPS, which welcomed the initiatives adopted by the Commission, while at the same time pointing out the need for further regulatory and/or legislative action at the national or European level.[70] The suggested measures were complemented by an Opinion by the Article 29 Working Party on smart metering.[71] In September 2018, the above-mentioned DPIA template was updated by the Smart Grids Task Force[72] to serve as guidance on data protection and privacy for data controllers and investors in smart grids.[73] Finally, the amended Electricity Directive[74] sets the functionalities smart meters must be equipped with in order to comply with the EU's data protection rules and at the same time to ensure the highest level of cybersecurity protection.[75]

The analysis under this subsection does not aim to provide a complete picture on smart grid personal data processing. Its only aim is to highlight the rich EU background in this regard and to suggest its applicability in the water sector as well. The use of smart devices is associated with significant risks for the protection of the users' personal data.[76] While it is true that the terms smart grids and smart meters have been introduced and extensively deployed by the energy sector and all definitions included in official EU documents make an explicit reference to energy suppliers and energy consumption,[77] given the anticipated increase in the use of smart technologies by water suppliers and network operators, the above terms may be, and have already been implemented, by analogy to the water suppliers.[78] Tellingly, the EDPS defines smart meters as 'an electronic device that records energy consumption and exchanges consumption data with energy suppliers, which is used for monitoring and billing. While this TechDispatch focuses on electricity smart meters, smart meters can also measure the consumption of other resources, such as natural gas or water'. Analogies have therefore already been identified in theory and are expected very soon to find full applicability in practice as well.[79]

How is security of personal data safeguarded in the context of the EU General Data Protection Regulation

Security of personal data is listed as one of the principles relating to processing of personal data under the EU's GDPR. Specifically, Article 5(1)(f) states that personal data shall be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality")'. According to Article 5(2) the controller shall be responsible for and be able to demonstrate compliance with all the principles of Article 5(1), including the principle of integrity and confidentiality.

The GDPR includes a separate section on security of personal data in Articles 32–34. Article 32 deals with the security of the processing and sets the controller's and the processor's obligation to implement technical and organisational measures to ensure a level of security including, among other things, the pseudonymisation and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in timely manner in the event of a physical or technical incident and a process for regularly testing the assessment and evaluation of the effectiveness of technical and organisational measures for ensuring the security of processing.

Another important parameter of security of personal data under the GDPR is the notification of a personal data breach to the supervisory authority. Data breach notifications are regulated by Article 33. A 'personal data breach' is defined in Article 4(12), as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'. When this happens controllers shall, according to Article 33(1):

> [w]ithout undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

70 See Opinion of the EDPS on the Commission Recommendation on preparations for the roll-out of smart metering systems, https://edps.europa.eu/sites/edp/files/publication/12-06-08_smart_metering_en.pdf.

71 See n 65.

72 The Commission set up a smart grids task force in 2019 to advise on policy and regulatory directions for the deployment of smart grids in Europe. See also https://www.edsoforsmartgrids.eu/policy/eu-steering-initiatives/smart-grid-task-force/.

73 Smart grids are energy networks that can automatically monitor energy flows and adjust to changes in energy supply and demand accordingly. When coupled with smart metering systems, smart grids reach consumers and suppliers by providing information on real-time consumption.

74 See Directive (EU) 2019/944 on common rules for the internal market for electricity and amending Directive 2012/27/EU.

75 Article 23(3) of the Directive states that: 'The processing of personal data within the framework of this Directive shall be carried out in accordance with Regulation (EU) 2016/679. Articles 20 b) and c) read as follows: b) the security of the smart metering systems and data communication shall comply with relevant Union security rules, having due regard of the best available techniques for ensuring the highest level of cybersecurity protection while bearing in mind the costs and the principle of proportionality, c) the privacy of final customers and the protection of their data shall comply with the relevant Union data protection and privacy rules'.

76 See also Vagelis Papakonstantinou and Dariusz Kloza 'Legal protection of personal data in smart grid and smart metering systems from the European perspective' in Sanjay Goel, Yuan Hong, Vagelis Papakonstantinou and Dariusz Kloza *Smart Grid Security* (Springer 2015).

77 See eg the Commission's Recommendation on preparations for the roll-out of smart metering systems, 2012/148/EU, definitions 3(a) and (b) of the directive on the definitions of smart grids and smart metering systems according to which smart grid means an upgraded energy network to which two-way digital communication between the supplier and consumer smart metering and monitoring and control systems have been added. Smart metering system means an electronic system that can measure energy consumption adding more information than a conventional meter and can transmit and receive data using a form of electronic communication.

78 On smart water grid and other smart water technology see also Aditya Gupta and others 'Smart water technology for efficient water recourse management: a review' (2020) 13(23) *Energies* 6268 https://www.mdpi.com/1996-1073/13/23/6268. See also Michele Mutchek and Eric Williams 'Moving towards sustainable and resilient smart water grids' (2014) 5(1) *Challenges* 123 https://www.mdpi.com/2078-1547/5/1/123/htm.

79 On the water gird concept see also Seongjoon Byeon and others 'Sustainable water distribution strategy with smart water grid' (2015) 7(4) *Sustainability* 4240 https://doi.org/10.3390/su7044240.

The obligation of notification burdens the processor as well, who shall notify the controller without undue delay after becoming aware of a personal data breach.[80] Paragraph 3 lists the minimum information the notification must contain, such as the nature of the data breach, the name and contact details of the data protection officer, the likely consequences of the personal data breach and the measures taken or proposed to be taken by the controller to address the personal data breach.

Finally, communication of a data breach to the data subject is regulated under Article 34. This obligation burdens the controller in any case where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons. The communication to the data subject shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in Article 33(2). Article 34(3) sets the conditions under which the communication to the data subject is not required: Article 34(3) reads as follows:

> The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met: (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

Water suppliers/network operators, as data controllers, need to implement appropriate technical and organisational measures to ensure an appropriate level of security. To assess what is the required level of security, they need to take into account the risks that are presented by the specific processing activities, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to their users' personal data. At the same time, they need to design and implement a data breach notification policy in order to comply with the notification obligations provided by the GDPR. In the same context, depending on the circumstances, the need to appoint a data protection officer and conduct a DPIA should always be evaluated and implemented in practice, if required.

DOES THE CURRENT REGULATORY REGIME RESPOND TO THE CHALLENGES OF SMART WATER MANAGEMENT? WHAT SHOULD THE NEXT STEPS BE?

Is a revision of the WFD from a cybersecurity perspective an actual option? Do the NIS and the ECI Directives cover the cybersecurity gaps?

As demonstrated above, the current regulatory regime on the water supply and wastewater sectors has been designed with a one-sided approach in mind that focuses mainly on securing clean and safe water for consumers. Consequently, protecting the water infrastructures against cyber threats and ensuring the availability and undisturbed operation of water services were not among the EU legislator's priorities when designing the sector-specific doctrine. At that time the focus was to put together the different water policies on water management and water protection with the intention of achieving good status of EU waters. This approach was reconfirmed recently when any thoughts on revising the WFD were officially abandoned by the Commission, which on 23 June 2020 announced that the directive and its 'daughters' would not be revised, but that the priority substances and the groundwater annexes might be updated.[81] The Commission pointed out that any efforts should focus on implementing and enforcing the directive. Even though it is not possible to be aware of the legislator's intentions and whether the anticipated revision would include any references to the protection of water facilities and services against cyber risks, the bottom line is that the European legislative bodies are of the opinion that the WFD still fulfils its purpose and, even if it has not yet proved its full potential, it is going in the right direction.[82]

In addition to this realisation, it would appear that any revision of the WFD in the cybersecurity direction would most likely not be feasible. When it was drafted its main purpose was to introduce a single piece of legislation on water management that would replace previously fragmented water policies. The good water status that the WFD aims to achieve is determined by the combination of its good ecological and chemical status. In this context, while it defines pollution as the 'direct or indirect introduction, as a result of human activity, of substances or heat into the air, water or land which may be harmful to human health or the quality of aquatic ecosystems',[83] such 'human activity' is not perceived to include cyber incidents but merely the accidental or even malicious human behaviours that have an adverse effect on the quality of water. The OECD further confirms this when, in its section on water risks, disasters and climate change, it refers to four major risks related to water, none of which includes cyber threats.[84] In addition, in 2000, when the directive entered into force, cyber awareness was still in its infancy, let alone in a sector that did not seem to be

80 See art 33(2) of the GDPR.

81 See Water Europe 'The Water Framework Directive will not be revised' https://watereurope.eu/the-water-framework-directive-will-not-be-revised/ and also EurEau 'European Commission decides not to revise the WFD' https://www.eureau.org/resources/news/456-european-commission-decides-not-to-revise-the-wfd#:~:text=The%20directive%20is%20the%20centrepiece,good%20ecological%20condition%E2%80%9D%20by%202027.&text=They%20will%20look%20into%20the,called%20'daughter%20directives.

82 The EU Water Legislation Fitness check concluded that: 'As for future challenges, this fitness check finds that the Water Framework Directive is sufficiently prescriptive with regard to the pressures to be addressed, and yet flexible enough to accommodate emerging challenges such as climate change, water scarcity and pollutants of emerging concern (e.g. microplastics and pharmaceuticals). A key area where there is room to improve and to achieve better results is on chemicals'. https://ec.europa.eu/environment/water/fitness_check_of_the_eu_water_legislation/index_en.htm.

83 See art 2(33) of the WFD.

84 The OECD identifies four major risks related to water: risk of too much, too little and too polluted water; and disruption to freshwater systems. In addition, lack of access to water supply and sanitation can be considered as another water-related risk.

affected by cyber threats. In this context, it is believed that any attempt to rewrite the directive from a cybersecurity perspective would require a total restructuring of its provisions, which would be both risky and, ultimately, unnecessary.

It seems, therefore, that a more 'traditional' approach has been adopted so far on identifying and addressing the current risks of water infrastructures and services. With sector-specific legislation excluded, any cyber concerns associated with the digitalisation of water services are left to be addressed by the cybersecurity regulatory framework, including the framework on critical infrastructures. As already mentioned above, both the NIS Directive and EU policy on the protection of critical infrastructures are applicable to the water sector, because water suppliers are listed among the entities that qualify as operators of essential services. Protection under the NIS Directive specifically is expected to increase as the proposal for a new NIS Directive includes the wastewater sector in its list of essential entities. In addition, the proposal for a new ECI Directive refers explicitly to the water sector, thus making the regime on the protection of European critical infrastructures directly applicable to water entities. Consequently, water utilities will be afforded a basic cybersecurity regulatory framework that provides them with adequate safeguards for the protection of their network and information systems against cyber risks. At the same time, however, both frameworks mentioned above represent a cross-sectoral approach, where no differentiation is made between sectors but the level of obligation is dependent only on the criticality of services provided. As the digitalisation of water management increases and consequently the water infrastructures and services gradually turn into a more attractive target for cyber attackers, the need for additional measures that would focus on the water sector specifically seems today more relevant. Several steps have already been taken in this direction in the energy sector, which, given the similarities of the two sectors, could pave the way for a more sectoral approach in the water industry as well.

The need for sector-specific initiatives in the water sector: the example of the energy sector as best practice

The Commission has, over recent decades, undertaken specific initiatives in an effort to make the energy sector more cyber resilient. It is true that energy infrastructures are among the most complex and most critical infrastructures, serving as the backbone of almost all economic and societal activities. It is also true that the energy sector has experienced some of the most serious cyberattacks in the recent past.[85] At the same time, it presents certain particularities that make the need for further action even more demanding. The Commission has identified three parameters that differentiate the energy sector from other critical services providers. These include real-time requirements, which in practice means that some energy systems react so fast that standard security measures do not suffice. Secondly, the energy systems can produce cascading effects, given that electricity grids and gas pipelines are strongly interconnected across Europe and well beyond the EU. Finally, many elements of the energy systems were designed and built well before cybersecurity considerations came into play. These elements now need to interact with the most recent state-of-the-art equipment for automation and control, such as smart meters or connected appliances without being exposed to cyber-threats.[86] With regard to this last parameter in particular, even though the integration of ICT in energy sector systems has been used for information exchange and automation for decades, their usage has increased dramatically in recent years, thus turning Europe's power grid into a 'smart grid'. A 2018 report prepared by the Commission on the deployment of smart meters in the EU found that close to 225 million smart meters for electricity and 51 million for gas will be rolled out in the EU by 2024. It is also expected that almost 77 per cent of European consumers will have a smart meter for electricity by 2024. About 44 per cent will have one for gas.[87]

The particularities of the energy sector together with its rapid digitalisation has led the EU to the conclusion that general cybersecurity strategies, even though they are accurate and up to date, need to be complemented by sector-specific cybersecurity measures. This is well depicted in the Commission's 2017 Joint Communication,[88] where energy is referred to as a sector that should be encouraged to develop its own approach.[89] In this context, in April 2019 the EU adopted a Recommendation on cybersecurity in the energy sector.[90] The Recommendation acknowledges the importance of sector-specific considerations at the EU level in the energy sector and suggests specific measures to address the issues related to cybersecurity.[91] Other sector-specific initiatives include the Regulation on measures to safeguard the security of gas supply[92] and the Regulation on risk-preparedness in the electricity sector. In particular, recital 7 of the second Regulation clearly states that 'This Regulation complements Directive (EU) 2016/1148 by ensuring that cyber-incidents are properly identified as a risk, and that the measures taken to address them are properly reflected in the risk-preparedness plans'. Finally, the Regulation on the internal market for electricity[93] and the Electricity

85 See Ecofys 'Study on the evaluation of risks of cyber-incidents and on costs of preventing cyber-incidents in the energy sector' (2018, by order of European Commission) ch 2 https://ec.europa.eu/energy/sites/default/files/evaluation_of_risks_of_cyber-incidents_and_on_costs_of_preventing_cyber-incidents_in_the_energy_sector.pdf.

86 See cybersecurity in the energy sector https://ec.europa.eu/energy/topics/energy-security/critical-infrastructure-and-cybersecurity_en.

87 See the Commission's final report on Benchmarking smart metering deployment in the EU-28, (December 2019) https://ec.europa.eu/energy/studies_main/final_studies/benchmarking-smart-metering-deployment-eu-28_en.

88 See the Commission's Joint Communication on resilience, deterrence and defence: building strong cybersecurity for the EU, JOIN(2017) 450 final.

89 See s 2.2 of the Communication.

90 See Commission Recommendation on cybersecurity in the energy sector, SWD(2019) 1240 final.

91 The Recommendation is accompanied by the Commission's Staff Working Document, SWD(2019) 1240 final. Chapter 3 of the document analyses the specificities of the energy sector (real-time requirements, cascading effects, legacy technology combined with new internet of things devices).

92 See Regulation (EU) 2017/1938 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010 [2017] OJ L280 (28 October 2017).

93 See Regulation (EU) 2019/943 on the internal market for electricity of 5 June 2019.

Directive (EU) 2019/944[94] complement the energy regulatory regime. A reference to the functionalities of smart metering systems in Article 20 of the directive and the inclusion of the promotion of cybersecurity and data protection in the tasks of the ENTSO[95,96] for electricity, are some indicative examples of how the sector-specific legislation is trying to keep up with the technological advances in the energy field.

Providing a thorough analysis of the energy regulatory framework to protect from cybersecurity risks is of course far beyond the scope of this article. However, a reference to the main initiatives that have been introduced by the EU in order to tackle the cybersecurity issues that have emerged owing to the wide use of smart devices and the digitalisation of energy services is considered essential as these initiatives could be used as guidance in the effort to ascertain how the water sector could respond to its imminent digitalisation. It is true that, until recently, sectors like water supply (e.g. water distribution and wastewater), were not seen as being as active as the energy sector about the creation of security guidelines and standards for ICS protection. It is also true that the water domain is characterised by a low level of maturity concerning the integration and standardisation of ICT technologies. However, as discussed above, this is changing rapidly as global water challenges make the need to develop and implement smart, cost-effective and efficient water management systems more imperative than ever. With this new reality in mind, the water industry will now have to give thought to securing its systems as they are part of the IoT landscape with all of its inherent security issues.[97]

In this context, the Commission is expected to work towards the definition of a regulatory strategy about the adoption of smart water technologies in coordination with relevant stakeholders and standard organisations to ensure smooth digitalisation of water services in the next decade.[98] The constantly increasing awareness on the vulnerabilities of the water systems to cyber risks is also depicted in a study that was prepared for the European Commission (its Directorate-General of Communications Networks, Content and Technology) by the ict4water.eu.[99] The study recognises that the water industry of the future will be smart and emphasises the need to 'define and deploy a group of actions for the development of Digital Water Services in the single market'.

As discussions are still at a premature level, this article, following the example of the energy sector, suggests some measures that could tackle the cybersecurity and personal data protection challenges that have already emerged in the water sector and which are anticipated to evolve at a rapid pace in the years to come. In this context, a first step would be for the regulatory bodies officially to recognise the applicability of the terms smart grids and smart meters in the water domain and to adopt, in cooperation with the industry, a clear definition of these terms, taking into account the particularities of their use in the water context. The publication of guidelines for the definition of smart water grids is listed among the requested actions towards digitalisation of the water sector of the Rolling Plan for ICT Standardisation.[100] Furthermore, a direct reference to the functionalities of smart water metering systems and the need to secure their conformity with cybersecurity and personal data protection rules, following the example of the energy sector, is considered essential. Clearing the landscape on water smart grids and meters would help the Commission, ENISA and all other organisations that are actively involved in the regulatory process to develop sector-specific measures.

Consequently, instead of trying to apply, by analogy, the existing guidelines on energy to the water sector, the existence of a clear set of rules that would explicitly address the smart water cybersecurity challenges would strengthen the market's confidence, raise the cyber awareness of all involved stakeholders and reinforce the consumers' confidence in water services. Given that the idea of revising the WFD has been abandoned, a legislative proposal that would embrace the digital transformation of the water sector and would include specific technical rules on the deployment of smart devices and specific safeguards that would protect the water infrastructures and the provision of smart water services against cyberattacks, could contribute to the strengthening of the market's digital character. ENISA should consider adding the water sector to its list of critical infrastructures and services. It is undisputable that the EU Cybersecurity Agency could greatly contribute to the development of a consistent cybersecurity framework for water providers and network operators by issuing guidelines and raising awareness among the market players, in the same manner as it has already done with other critical sectors.

Security by design in smart devices: cybersecurity certification and standardisation and their applicability in smart water management

The constantly increasing digitalisation of our daily lives and the expanded use of smart devices in many different human activities have made security by design and by default an important tool in the effort to achieve a high level of cyber resilience. The need to have security built into smart products and services from the start has been identified by many European bodies as imperative. The Cybersecurity Act states in its recital 12 that:

> Organisations, manufacturers or providers involved in the design and development of ICT products, ICT services or ICT processes should be encouraged to implement measures at the earliest stages of design and development to protect the security of those products, services and processes to the highest possible degree, in such a way that the occurrence of

94 See also https://ec.europa.eu/energy/sites/default/files/documents/eecsp_report_final.pdf.

95 The European Network of Transmission System Operators for Electricity.

96 See art 30(1)(n) of the directive.

97 On the cybersecurity shift in the water sector see also Amin Rasekh and others 'Smart water network and cyber security' (2016) 142(7) *Journal of Water Resources Planning and Management* 1.

98 See Rolling Plan for ICT Standardisation 'Water management digitalisation' https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/water-management-digitalisation.

99 See ict4water.eu report on Digital Single Market for Water Services Action Plan https://ec.europa.eu/futurium/en/system/files/ged/ict4water actionplan2018.pdf.

100 The concept of the smart water grid is expected to be developed in the framework of ICT4Water cluster running projects. Many standard organisations like ETSI, CEN/CENELEC, AIOTI, OGC, OpenFog and BVDA are expected to contribute in coordination with the EC.

> cyberattacks is presumed and their impact is anticipated and minimised ('security-by-design').

The important role that ENISA will play in this effort is identified in recital 41 of the Act, where it is stated that: 'ENISA should play a central role in accelerating end-user awareness of the security of devices and the secure use of services, and should promote security-by-design and privacy-by-design at Union level'. In the same context, the EU's new Cybersecurity Strategy for the Digital Decade recognises that:

> the EU's critical infrastructure and essential services are increasingly interdependent and digitised. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be secure-by-design, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered.[101]

Security by design is therefore a necessary condition in order to keep network systems free of vulnerabilities and resilient to attacks at an early stage through the integration in their architecture design of security features and requirements. As elaborated in the previous sections of this analysis, smart water management is based on the use of smart devices, such as smart grids and smart meters. In the coming years it is anticipated that the integration of ICT in the water networks and services will increase exponentially. Deploying security by design is expected to play an essential role in ensuring a standard level of security for smart devices used by the water utilities. To this effect all involved stakeholders in the water industry are anticipated to work together in order to design a set of technical functionalities and minimum security requirements to be built into the architecture of smart meters and grids. Following the example of the Smart Grid Task Force, which has issued key recommendations for standardisation, consumer privacy and security for the deployment of smart grids,[102] the ICT4Water cluster could undertake similar initiatives. ENISA could also contribute to this task by issuing guidelines targeting water smart grids and meters directly.

In order to ensure a standard high level of cybersecurity for ICT products and services, operators and manufacturers of smart devices and developers of smart services need a specific regulatory framework. Cybersecurity certification and standardisation can provide great assistance to businesses during the design and manufacture process. As set out in the Cybersecurity Act, currently the cybersecurity certification of ICT products, ICT services and ICT processes is used only to a limited extent and, when it does exist, it mostly occurs at Member State level or in the framework of industry-driven schemes. As a result, at the moment, there are various different security certification schemes for IT products around the EU.[103] The Act aims to address this fragmentation by introducing a new cybersecurity certification framework for ICT products, ICT services or ICT processes. The Commission is already working on an EU-wide certification framework,[104] with ENISA at its heart.[105] To date ENISA has published a report on the functional requirements for a potential ICT security certification scheme for a widely understood healthcare sector. Furthermore, it has prepared the EUCC scheme[106] and it has launched a public consultation on the draft version of the EUCS candidate scheme.[107] In February 2021, ENISA welcomed the Commission's request for the preparation of the new candidate cybersecurity certification scheme on 5G. Even though the Commission is not currently working on an ICT security certification scheme for the water sector, a proposal that would tackle digital water management services including smart grids and smart meters deployed in the water sector would contribute to the process of their certification based on cybersecurity requirements that have been horizontally approved at the EU level.[108]

The benefits of standardisation in cybersecurity are undisputable and include, among others, harmonisation of terminology, consistency between different manufacturers, conformity of products with specific requirements, enhancement of users' trust in the products' safety, performance checking and security evaluation, to mention only a few. Therefore, standardisation has an essential role to play in increasing interoperability of new technologies within the digital single market.[109] The Commission is setting up ICT standardisation priorities for the digital single market, having published a Communication on ICT Standardisation.[110] The Commission has identified five priority domains where it considers ICT standardisation most urgent for the completion of the digital market, cybersecurity being one of them.[111] The EU Rolling Plan for ICT Standardisation is an essential instrument in this regard.[112] The rolling plan is built around the five priority domains set in the Communication and in addition to that it has identified a total of 165 actions grouped into four thematic areas: the fourth area (entitled sustainable growth) includes a subcategory on smart grids and smart

101 See Commission's Joint Communication on the EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020)18 final, s 1.

102 On the SGTF recommendations and other initiatives see https://www.edsoforsmartgrids.eu/policy/eu-steering-initiatives/smart-grid-task-force.

103 See recital 67 of the Act.

104 See European Commission 'The EU cybersecurity certification framework' https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

105 The role of ENISA in the area of the EU cybersecurity certification framework is 'to pro-actively contribute to the emerging EU framework for the ICT certification of products and services and carry out the drawing up of candidate certification schemes in line with the Cybersecurity Act, and additional services and tasks'. See also ENISA 'EU cybersecurity certification framework' https://www.enisa.europa.eu/topics/standards/certification.

106 The EUCC Candidate Scheme (Common Criteria based European candidate cybersecurity certification scheme) looks into the certification of ICT products' cybersecurity, based on the common criteria, the common methodology for information technology security evaluation and corresponding standards, respectively, ISO/IEC 15408 and ISO/IEC 18045.

107 See ENISA's EUCS-Cloud Services Scheme ((European Cybersecurity Certification Scheme for Cloud Services) (December 2020).

108 ENISA has issued a study on smart grid security Recommendations, 2012 and a report on Smart Grid Security Certification in Europe (2014).

109 Regulation 1025/2012 on European standardisation sets the legal framework in which the actors in standardisation (the European Commission, European standardisation organisations, industry, SMEs and societal stakeholders) operate.

110 See the Commission's Communication on ICT Standardisation Priorities for the Digital Single Market, COM(2016) 176 final. See also European Commission 'Standards' https://ec.europa.eu/digital-single-market/en/standards.

111 The other four are the IoT, big data technologies, 5G communication and cloud computing.

112 See the rolling plan for ICT standardisation 2020 https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020.

metering as well as on water management digitalisation. Specifically the rolling plan states that: 'the development of system standards is a key enabling factor for smart water solutions that ensures interoperability of solutions through promoting common meta-data structures, standard protocols and interoperable (open) interfaces instead of proprietary ones'. The main goal, according to the plan, is 'to foster the creation of a Digital Single Market for water services to promote the transition of the ICT technologies and standards towards large pilot scale and to expand the market uptake of the technologies'.[113]

Information sharing on cyber incidents in the water sector

Information sharing is a key element in cybersecurity as it enables all stakeholders to acquire a detailed view on the current cyber threats landscape, to identify possible trends, and to take the appropriate preventive measures. The Commission has undertaken several actions to strengthen the exchange of information on cyber incidents and cyber threats. One of the most important initiatives is the establishment of the Information Sharing and Analysis Centres (ISACs).[114] ISACs are non-profit organisations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) and allow two-way sharing of information between the private and the public sector about root causes, incidents and threats.[115] Their role in creating the necessary trust for sharing information between private and public sector was identified in the EU's Cybersecurity 2017 Strategy.[116] Both the Cybersecurity Act and the NIS Directive promote the creation of ISACs.[117] Different models of ISACs exist in several EU Member States.[118] Some are country-focused, while others are sector-specific ISACs that encourage cooperation on the sectorial level of critical infrastructure or essential/vital sectors; in addition, there are international ISACs that bring together multi-stakeholder members from Europe and third countries.[119]

As regards sector-specific ISACs in particular, some first steps have been taken in respect of some critical sectors such as aviation, through the creation of the European Centre for Cybersecurity in Aviation, and energy, through the creation of the European Energy Information Sharing and Analysis Centre.[120] The new cybersecurity strategy repeats the belief of the valuable contribution of ISACs to information exchange between multiple stakeholders on cyber threats.[121] The Commission in its turn aims to strengthen the position of ISACs with the support of ENISA through an acceleration in particular with regard to sectors providing essential services. ENISA is already contributing to this effort by offering advice and expertise in several European initiatives regarding the development of ISACs. In October 2020, ENISA launched ISAC in a box, a comprehensive online toolkit to support the establishment, development and evaluation of ISACs.[122] Smart water management and the deployment of smart devices for the provision of water services increase the risk of cyber-attacks that target the water utilities. Even though the water sector has not yet been digitalised to the extent the energy sector has, where information sharing initiatives have already been adopted, smart water is expected to grow significantly in the near future. Therefore, it is believed that the Commission should, with ENISA's support, put in its agenda the development of an ISAC for the water sector. By sharing information, analysing cyber threats and evaluating counter-measures to respond to such threats, the water sector will undoubtably acquire a great advantage in making smart water networks and services more resilient to cyberattacks.

CONCLUSION

The digitalisation of the water sector is moving at a fast pace with smart water management systems being deployed by a constantly increasing number of water suppliers and network operators. However, turning the management of water 'smart', through the use of smart devices, such as smart meters and smart water grids, comes at a price. The integration of ICT in the water systems and networks makes the provision of water services more efficient and sustainable; however, at the same time it makes water facilities more vulnerable to cyberattacks. The current regulatory framework on water management and water safety, after almost five decades of development, has reached a certain level of maturity.

113 See the rolling plan for ICT standardisation 'Water Management Digitalisation' https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/water-management-digitalisation.

114 ISACs were originally created in the USA. In 1997, after the first terrorist attacks on the World Trade Center (1993) and Oklahoma City (1995), President Clinton appointed the President's Commission on Critical Infrastructure Protection (PCCIP). Its objective was to identify the possibility of cooperation between public and private sector so that the US critical infrastructure could be properly protected. Chaired by Robert T. Marsh, the Commission presented the so-called 'Marsh report' with many recommendations about raising the level of critical infrastructure protection in the US. One of its main recommendations was to establish information sharing and analysis centers (ISACs), so as to build and strengthen cooperation between public administration and the industry.

115 At the European level, sectoral information sharing and analysis centres (ISACs) and corresponding CSIRTs can play a key role in preparing for and responding to cyber incidents. See European Commission 'Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry' COM(2016) 410 final.

116 See the Commission's Joint Communication on resilience, deterrence and defence: building strong cybersecurity for the EU, JOIN(2017) 450 final.

117 See recital 29 of the Act.

118 In the Netherlands, for instance, ISACs are established by the Government's National Cyber Security Centre on a sector-by-sector basis (water, energy, finance etc). In the United Kingdom, a very similar setup has been introduced, organised by the government's Centre for the Protection of National Infrastructure (CPNI). In Germany, UP KRITIS is a large co-regulatory initiative in which critical infrastructure organisations participate (both private and public entities). Within UP KRITIS, information is shared based on the Traffic Light Protocol (TLP) as the information cannot always be made public. Information is shared via emails and standard templates provided by the Federal Office for Information Security (BSI). See also ENISA's report on Information Sharing and Analysis Centres (ISACs) of 2017.

119 EU FI–ISAC – a European ISAC that serves the financial sector, EE–ISAC – a European ISAC created in 2015 that serves the energy sector. European ISAC in the Aviation sector – an ISAC under creation, initiated in February 2017 by the private sector in cooperation with ENISA and EASA (European Union Aviation Safety Agency).

120 The European Energy – Information Sharing Analysis Centre (EE–ISAC) helps utilities to improve the cyber security and resilience of their grid by enabling trust-based data and information sharing. EE–ISAC was created in 2015. The EE–ISAC provides a platform for members to share information on cyber security and cyber resilience in the energy sector. See also https://www.ee-isac.eu/.

121 See s 1.2. of the EU Strategy.

122 See ENISA's ISAC in a Box Toolkit https://www.enisa.europa.eu/news/enisa-news/isac-in-a-box.

However, it adopts a more traditional approach in terms of addressing water risks and water security without tackling the cybersecurity concerns the digitalisation of the water domain raises. As the water sector cyber threat landscape is evolving, the main question that arises is whether water facilities are adequately secured against cyber-attacks within the existing sector-specific and cyber-security regulatory frameworks.

The growing number of cyber incidents that target critical infrastructures and their network and information systems has motivated the EU to develop a number of legislative instruments to secure them against cyber risks. The NIS Directive, the ECI Directive and the protection regime on critical infrastructures create a satisfactory security framework within which critical infrastructures and operators of essential entities may securely operate. The cybersecurity framework finds full applicability in the water sector as water utilities qualify as critical infrastructures and operators of essential services within the context of both legislative instruments. In addition, the GDPR offers a comprehensive framework for the protection of the personal data of the users of water services, thus addressing the security concerns that arise from the possibility of a security data breach.

Nevertheless, as these instruments are horizontal, the need for additional sector-specific measures should be examined. Following the much more mature – at least, in terms of both digitalisation and cyber awareness – example of the energy sector, this article suggests specific initiatives that could accelerate the cyber resilience of the water sector and help water suppliers and water network operators to achieve a greater level of cyber resilience for their networks and services. The suggested measures include an official reference by the European bodies to smart water grids and smart water meters, as well as the introduction of specific guidelines and perhaps a legislative instrument that would address the cyber-security concerns that arise from the use of smart devices by the water entities. Additionally, the implementation of the security by design principle in the manufacture of smart water devices, the introduction of specific standards and security certification schemes that would directly address smart water grids and smart water services, as well as the reinforcement of information sharing initiatives on cyber incidents in the water domain are some initiatives that could contribute to building a cyber secure water industry. However, before even starting to evaluate the effectiveness and applicability of these measures, all stakeholders in the water sector need to realise that the radical transformation of water services makes their alertness and cyber awareness necessary in order to be able to respond to the new challenges that are brought within the new digitalised water landscape.