PARLIAMENTARY DEBATES

HOUSE OF COMMONS
OFFICIAL REPORT

First Delegated Legislation Committee

DRAFT NETWORK AND INFORMATION SYSTEMS (EU EXIT) (AMENDMENT) REGULATIONS 2021

Monday 13 December 2021

No proofs can be supplied. Corrections that Members suggest for the final version of the report should be clearly marked in a copy of the report—not telephoned—and must be received in the Editor's Room, House of Commons,

not later than

Friday 17 December 2021

The Committee consisted of the following Members:

Chair: Mr Peter Bone

† Blunt, Crispin *(Reigate)* (Con)
Day, Martyn *(Linlithgow and East Falkirk)* (SNP)
Ellwood, Mr Tobias *(Bournemouth East)* (Con)
† Elmore, Chris *(Ogmore)* (Lab)
† Evennett, Sir David *(Bexleyheath and Crayford)* (Con)
† Fabricant, Michael *(Lichfield)* (Con)
† Fovargue, Yvonne *(Makerfield)* (Lab)
† Jones, Mr David *(Clwyd West)* (Con)
Keeley, Barbara *(Worsley and Eccles South)* (Lab)
† Lloyd, Tony *(Rochdale)* (Lab)
† Lopez, Julia *(Minister for Media, Data and Digital Infrastructure)*
† Morden, Jessica *(Newport East)* (Lab)
† Nici, Lia *(Great Grimsby)* (Con)
Osamor, Kate *(Edmonton)* (Lab/Co-op)
† Tomlinson, Michael *(Lord Commissioner of Her Majesty's Treasury)*
† Wakeford, Christian *(Bury South)* (Con)
† Watling, Giles *(Clacton)* (Con)

Huw Yardley, *Committee Clerk*

† attended the Committee

First Delegated Legislation Committee

Monday 13 December 2021

[Mr Peter Bone *in the Chair*]

Draft Network and Information Systems (EU Exit) (Amendment) Regulations 2021

4.30 pm

The Chair: I can confirm that we are definitely quorate. Before we begin, may I remind Members that they are expected to wear face coverings and to maintain social distancing as far as possible? This is in line with current Government guidance and that of the House of Commons Commission. Please give each other and members of staff space when seated and when entering and leaving the room. I remind Members that they are asked by the House to have a covid lateral flow test twice a week if they are coming on to the parliamentary estate. This can be done either at the testing centre in the House or at home. Members should send their speaking notes by email to hansardnotes@parliament.uk. Similarly, officials in the Gallery should communicate—*[Interruption.]* Yeah, maybe not. I call the Minister.

4.31 pm

The Minister for Media, Data and Digital Infrastructure (Julia Lopez): I beg to move,

That the Committee has considered the draft Network and Information Systems (EU Exit) (Amendment) Regulations 2021.

The regulations were laid in draft before the House on 26 October. This short but very important statutory instrument makes technical corrections to the UK's network and information systems legislation, which arose as a result of the UK leaving the EU. These corrections will allow the Information Commissioner, in her role as the regulator for digital services providers, to be informed of important cyber incidents affecting online marketplaces, online search engines and cloud computing services in our country.

Before moving on to the amendment at hand, it is important that we first consider the context that we find ourselves in. The NIS regulations were introduced in the UK in 2018, implementing the EU's 2016 directive on security of network and information systems. The regulations provide a legal framework to protect the network and information systems of essential and digital services. They do this by directing operators of essential services and digital service providers to take steps to protect—against cyber-attack and physical fault—the security of those systems that their services rely on.

Beyond ensuring the security of their network and information systems, these organisations have other duties as well. One of the most significant, and the most relevant for this statutory instrument, is the duty to report to their regulator incidents that have a substantial impact on their services. Such reports are critical to the regulator's ability to react and to implement the NIS legislation. The regulator can then provide advice, report the incident to the national technical authority—in this case the National Cyber Security Centre—or take enforcement action if appropriate.

Michael Fabricant (Lichfield) (Con): Does my hon. Friend think that these changes not only fill a gap from our leaving the EU but create an environment whereby we can perform better than if we had remained in the EU?

Julia Lopez: I would like to provide my hon. Friend with a very positive story about Brexit through these regulations, but this is quite a technical and narrow change. When it comes to his ambitions, we have a much more ambitious agenda in the coming year or so.

Without the information required, the regulator is not aware of the incident, and citizens and businesses relying on that service are affected for longer. The threshold for what qualifies as a reportable incident for the majority of the six sectors is set in statutory guidance by the relevant regulators. Only one sector—digital service providers, which are regulated by the Information Commissioner—has its set in legislation. All other regulators are able to react to the changing circumstances and amend the thresholds as necessary.

The Information Commissioner is limited by that retained EU law. That is due to how the NIS directive was established. In the EU, digital service providers are regulated at Union level, rather than at individual country level. For that reason, the thresholds that establish whether an incident has had a substantial impact on the security of a network and information system were not left to individual member states to establish, as is the case with all other sectors. These were set out in a Commission implementing regulation, which harmonised the rules across the whole EU. Following our withdrawal, it remained embedded in the UK statute book by virtue of the European Union (Withdrawal) Act 2018. Therefore, the thresholds remain at the level suitable for the EU, which has a population of 500 million, not for the just under 70 million of our own population. That means that they are unable to be changed to reflect our new position as an independent country outside the EU.

Parameters such as the amount of users impacted or user hours lost from an incident are set far too high currently for the UK, and considerations relating to impacts on EU citizens are not appropriate for our own NIS legislation. The Information Commissioner has received only one report since we left the EU. That is not surprising if an incident must have a noticeable impact on an economy the size of the EU in order to be reported in the UK. Without incident reporting, the commissioner will not have an understanding of the threats to and impacts on the sector, and will not be able to identify threats, provide guidance or take enforcement action if appropriate. For the NIS regulations to remain effective in protecting the essential services provided, we have to be able to set the reporting thresholds at a suitable level for our own country. This statutory instrument is designed to resolve that issue by removing those deficient provisions in retained EU law and allowing the Information Commissioner to set the thresholds to a level that effectively reflects our position and size.

The enabling provisions under section 8 of the 2018 Act allow changes to be made to rectify EU exit-related deficiencies only. I am content that the amendments made in this statutory instrument do not introduce new policy, although we have ambitions in that regard; rather, they are meant to ensure that the original policy objective is achieved. The Information Commissioner has already carried out a consultation on the level of thresholds to be set to represent the UK market, and

the practice of setting appropriate thresholds for reporting is already in place for every other competent authority. This statutory instrument will bring digital service providers in line with all other operators of essential services in the UK.

Additional amendments in the statutory instrument cover textual changes as a consequence of the UK's withdrawal from the EU. This includes a requirement for digital services providers to consider the geographic impact of an incident in relation to the UK rather than across the UK. The NIS regulations form part of the Government's toolkit to protect digital services, which citizens rely on in their day-to-day lives, and help to support the functioning of the digital and physical economies. That is why it is essential that we maintain the framework for protecting our essential services and deter those who seek to act in a subversive manner towards them. For those who do unfortunately fall victim, it is necessary to provide support in guidance. To do this, competent authorities have to be informed of such incidents.

This statutory instrument incorporates much-needed amendments to the NIS legislative framework, which will lead to increased security of digital service providers and their network and information systems. Although the amendments are minor and technical in nature, they are none the less critical for maintaining the effectiveness of the NIS legislation and for providing the Information Commissioner with the right information to support digital services in the UK. I commend the regulations to the Committee.

4.37 pm

Chris Elmore (Ogmore) (Lab): It is a pleasure to serve under your chairmanship, Mr Bone. May I start by saying that I hope that in the months ahead I can work constructively with the Minister in my new role? I accept that there will be times when we will disagree, but I hope that she will always know that that will be on matters of policy and never, ever personal.

We do not oppose the regulations, which address EU exit-related deficiencies in the retained EU legislation that regulates the security of network and information systems of core UK service providers. There are no specific points that I would like to raise in direct relation to the regulations, which seek to recognise the UK's position outside the European Union and the necessary legislative changes that need to be addressed. I also note that no concerns were raised by the Secondary Legislation Scrutiny Committee. I would, however, like to make some more general observations on the SI itself, and I would be grateful to the Minister if she could answer my questions either now or in writing.

The prevalence of cyber-related attacks has only grown in recent years. In August it was reported that nine cyber-attacks on the UK's transport infrastructure were missed by mandatory reporting laws due to the reporting thresholds being so high. To add further concern, the Government were alerted to those attacks only because the information was given voluntarily.

It is clear, given the UK's position outside the European Union, that changes need to made to the setting of parameters for digital service providers, which is currently still retained in EU legislation. However, given that it has been over a year since the end of the transition period, there is concern that we are only now finding time to debate issues relating to our national cyber infrastructure. As noted in the SI, having the EU set the parameters for incident reporting by digital service providers does not work effectively for the UK as a stand-alone nation, as the Minister has touched on. The main issue is that the reporting threshold for EU nations is too high to trigger reporting in the UK. The Opposition recognise and agree that changes need to be made to reflect the UK outside the EU. We cannot have a situation where the Information Commissioner is not alerted to cyber incidents that have caused disruption to the activities of digital service providers, many of which are crucial to the smooth, day-to-day running of society.

The Minister has said that this statutory instrument is not going to be used as part of any future relationship agreement with the European Union. Cyber-attacks and breaches of digital infrastructure are not unique to one nation. Digital is a shared commodity, not bound by physical borders. Could the Minister elaborate on what discussions are being had with European neighbours on joint working reporting of cyber-attacks against digital service providers? Although I recognise the need for the UK to have its own reporting mechanism, close collaboration on shared security issues remains crucial.

Michael Fabricant: Does the hon. Gentleman agree that this is not just about the European Union? The United Kingdom has just entered into an agreement with the state of Israel, which is perhaps, some would argue, the most advanced country in the world on cyber-security. Does he welcome that?

Chris Elmore: For the avoidance of doubt and for the record, I do welcome the collaborative agreement. Clearly, the issue of cyber-security applies beyond the European Union; in fact, it affects all nations around the world. What we are discussing today, however, as the Minister has said, is the need to improve the current state of play from when we left the European Union—the transition period ended over a year ago. Of course, I agree entirely that the more relationships we have in terms of improving our data and cyber-security, the better.

Michael Fabricant: Good answer.

Chris Elmore: I am delighted.

Given that the proposed changes will increase the scope and responsibilities of the Information Commissioner's Office, does the Minister believe that the Information Commissioner has enough staff and wider resource to complete those duties? The explanatory memorandum states that the next post-implementation review of the NIS regulations will take place by May 2022 and that subsequent reviews will take place no later than every five years. Given the rapid pace of change in innovation in digital services, will the Minister seek to ensure that reviews take place no later than every two years, to keep pace with any change in the sector?

Finally, the explanatory memorandum states:

"The legislation does not apply to activities that are undertaken by small businesses."

I am sure that all Members present recognise that the pandemic has accelerated the growing trend for more and more businesses to move online, especially small

[Chris Elmore]

business owners. What discussions are taking place to protect small businesses that are classed as digital service providers but are not recognised by the ICO as relevant data service providers, as they continue to grow in number? Beyond that, as I have said, we do not object to the regulations.

4.42 pm

Julia Lopez: I thank members of the Committee for attending and for their patience in debating the regulations. I also welcome the hon. Member for Ogmore to his position. I am very glad that he supports the regulations, and I very much appreciate the warm welcome he gave me. I look forward to working with him collaboratively where we can and to addressing his concerns when he raises them.

I assure the hon. Gentleman on our general approach to cyber-security. We entirely understand how important this area is. To that end, this week we are launching a new national cyber strategy, which is a whole-of-Government approach but also a whole-of-society approach. Huge efforts are going to be required by each of us as citizens; otherwise, any vulnerability in the system will have an impact on all of us. As we have seen during the pandemic, more aspects of our lives have gone online, and with that comes a consequent risk.

I completely agree with the hon. Gentleman on the importance of joint reporting and collaboration. We held the future tech forum at the Science Museum a couple of weeks ago, and we started some of those discussions with ministerial counterparts in EU countries. There was an EU representative present and I look forward to working collaboratively with them.

My hon. Friend the Member for Lichfield was absolutely right to refer to the importance of the relationship with Israel. I met the ambassador when I was at the Cabinet Office and we talked about where we can collaborate more closely when it comes to cyber-technology, because it is such an important area. It is the area of the future, where I fear we will be fighting many of tomorrow's battles.

We have been assured that the ICO has the resources to deal with the extra reporting. I also say to the hon. Member for Ogmore that we will consult on NIS regulations early in the new year. We will also be looking at expanding the list of people that this applies to. I entirely agree with him about the importance of dealing with small businesses, which are going to be holding increasing amounts of risk. We are doing a huge number of things in that regard, including improving the skills base from which they can recruit cyber expertise and introducing a new royal charter so that people can be assured of the cyber expertise that individuals hold. At the moment, that is a very messy landscape. I hope that that assures the hon. Gentleman on some of the initiatives that we are working on. If he has any further questions, I shall be happy to engage with him. I commend the regulations to the Committee.

Question put and agreed to.

4.44 pm

Committee rose.