EU Internet Forum adopts “Crisis Protocol” to prevent viral spread of certain kind of content online

IRIS 2020-1:1/17

Melinda Rucz
Institute for Information Law (IViR)

At its fifth annual meeting on 7 October 2019, the EU Internet Forum was devoted to the EU Crisis Protocol. The aim of the Protocol is to facilitate a rapid response mechanism to tackle the viral spread of terrorist and other violent extremist content online.

The European Commission set up the Internet Forum in 2015 in response to the alarming increase in the use of the Internet by terrorists to spread extremist propaganda. Acknowledging the crucial role that the Internet can play in the fight against incitement to violence, the Internet Forum pledged to bring together representatives of the technology industry, national governments and Europol to coordinate efforts against the online spread of terrorist content. Following the terrorist attack in New Zealand in March 2019, leaders of numerous national governments and the technology industry adopted the “Christchurch Call”, committing to eliminate terrorist and violent extremist content online (see IRIS 2019-7/2). The then president of the European Commission, Jean-Claude Juncker, declared at the time that an EU Crisis Protocol would be adopted by the Internet Forum by way of contributing to the global efforts prompted by the Christchurch Call.

The primary function of the Crisis Protocol is the facilitation of a rapid and coordinated cross-border response mechanism to contain the spread of terrorist content online. The European Commission, member states and various online service providers – including Facebook, Twitter, Google, Microsoft, Dropbox, JustPaste.it and Snap – have signed up to coordinate crisis management within the framework of the Protocol. The response mechanism is comprised of four steps. Firstly, on the basis of geographical reach and the speed of the spread of online content, an incident is identified as a crisis. After this, the relevant stakeholders, such as the affected member states and online service providers, are notified of the existence of the crisis. At this stage, Europol may coordinate notifications if multiple member states are affected. Subsequently, the relevant national law enforcement authorities and online service providers share (on a voluntary basis) real-time information about the online content concerned. On the basis of that information exchange, the law enforcement authorities and online service providers will coordinate efforts by drawing up operational plans, sharing hashtags and URLs, and maintaining a crisis log. At the last stage, a post-crisis

report is prepared in which all the actors that were involved in the management of the crisis assess the response and identify elements that can be improved upon in the future.

Furthermore, the Crisis Protocol emphasises the subsidiary nature of the response mechanism. The Protocol only applies in exceptional situations, when national crisis management procedures prove insufficient. Additionally, the Crisis Protocol highlights the need for an effective crisis communication method and lays down certain principles for this purpose. Specifically, under the Protocol procedure, the public, the media and other relevant stakeholders are kept informed about steps to alleviate the crisis throughout in order to ensure that the public is reassured that the appropriate steps are being taken, to mitigate any tensions and to pre-empt the spread of disinformation.

European Commission, Fighting Terrorism Online: EU Internet Forum committed to an EU-wide Crisis Protocol, 7 October 2019

https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6009