European Law Blog

EU sanctions against cyber-attacks and defense rights: Wanna Cry?

Franck Dumortier Paul de Hert Vagelis Papakonstantinou

European Law Blog

Published on: Sep 28, 2020

URL: https://europeanlawblog.pubpub.org/pub/eu-sanctions-against-cyber-attacks-imposed-and-defense-rights-wanna-cry

On July 30th 2020, within the framework of the Common Foreign and Security Policy (CFSP), the Council of the European Union has imposed its first ever "targeted restrictive measures" against six Chinese and Russian individuals as well as three legal entities – two located in the aforementioned countries and one in North Korea – for their involvement in significant cyber-attacks or attempted cyber-attacks against the EU or its Member States. These include cyber-attacks known as 'WannaCry', 'NotPetya', and 'Operation Cloud Hopper' and the attempted cyber-attack against the OPCW (Organisation for the Prohibition of Chemical Weapons).

This reaction for the first time materializes the cyber sanctions regime which was adopted in 2019 in order to operationalize "the Cyber Diplomacy Toolbox" for countering threats to international peace and security in the cyberspace. In addition to common diplomatic tools such as preventive, cooperative and stability measures, this framework allows the Council to impose targeted sanctions to State or non-State actors with the aim to respond to and deter significant cyber-attacks, "including in case of malicious cyber activities that do not rise to the level of internationally wrongful acts but are considered as unfriendly acts". According to the Council, such targeted restrictive measures should be differentiated from the attribution of responsibility for cyber-attacks to a third State which is a sovereign political decision every Member State is free to make on a case-by-case basis. The aim of restrictive measures imposed by the EU is to bring about a change in policy or activity by the target country, part of country, government, entities or individuals. However, as highlighted by Yuliya Miadzvetskaya, "the practice shows that a vast majority of cyber-attacks with high impact consequences, such as StuxNet, WannaCry and NotPetya, were orchestrated at the request and with the support of governments and not just by some random hacktivists". Hence, in practice, the delimitation between attribution of responsibility to a State and targeted measures imposed to individuals potentially sponsored by such State is rather superficial. Of course, the provisions of the Directive on Attacks against Information Systems, including its penalties, would be applicable in the case of criminal actors without significant ties to a State sponsor.

Concretely, the Council's Decision lists natural persons and legal entities "held responsible for, provided support for or were involved in, or facilitated cyber-attacks or attempted cyber-attacks"". Consequently, in principle, the listed persons and entities must be prevented to enter the EU territory, all of their funds and economic resources are being frozen and it is forbidden to make funds available to them.

Defense rights?

Due to its substantial negative impacts, the listing of targeted persons and entities must respect fundamental rights, in particular the right to an effective remedy and to a fair trial, but also the right to the protection of personal data of natural persons should, for example, a malicious cyber activity be wrongly attributed.

As held by the European Court of Justice in the *Kadi I* case, "the Community judicature […] must ensure the full review of the lawfulness of all Union acts in the light of the fundamental rights forming an integral part of the European Union legal order" (para.326. In *Kadi II*, the Court further detailed that the right of defense

"includes the right to be heard and the right to have access to the file, subject to legitimate interests in maintaining confidentiality" (para.99). As for the right to a fair trial, it "requires that the person concerned must be able to ascertain the reasons upon which the decision taken in relation to him is based, either by reading the decision itself or by requesting and obtaining disclosure of those reasons, without prejudice to the power of the court having jurisdiction to require the authority concerned to disclose that information, so as to make it possible for him to defend his rights in the best possible conditions and to decide, with full knowledge of the relevant facts, whether there is any point in his applying to the court having jurisdiction, and in order to put the latter fully in a position to review the lawfulness of the decision in question" (para.100. Hence, the decision to subject a person or entity to targeted restrictive measures requires clear criteria, tailored to each specific case, for determining which persons and entities may be listed, which should also be applied for the purpose of removal from the list. Moreover, the Council is bound by the obligation to state reasons laid down in Article 296 TFEU which entails that the statement of reasons identifies "not only the legal basis of that measure but also the individual, specific and concrete reasons why the competent authorities consider that the person concerned must be subject to restrictive measures" (*Il-Su Kim & KNIC*, para. 70).

Such a requirement to sufficiently substantiate by evidence the reasons invoked to include persons and entities into a list to whom restrictive measures are imposed is not easy to combine with the difficulty to attribute complex and quasi-anonymous cyber-attacks with a certain degree of certainty. Therefore, the Council considers that "attribution could be established, based on an analysis of technical data and all-source intelligence, including on the possible interests of the aggressor". However, revealing such evidence could potentially imply the disclosure of sensitive information touching upon the security of the EU or of its Member States. Therefore, "the entitlement to disclosure of evidence as part of the rights of the defense is not an absolute right" but imposes to "weigh the public interest in non-disclosure against that of the accused in having sight of the material" (*Jasper v. UK*, para. 52). In cases where evidence has been withheld from the defense on public interest grounds, it is up to national courts to decide whether or not such non-disclosure was strictly necessary. In brief, for the person concerned, accessing the clear reasoning behind restrictive measures on the basis of the right to a fair trial can practically imply long and heavy judicial proceedings.

Better alternatives in the toolbox?

For this reason, an interesting alternative would be to invoke the right of access to personal data necessary for the correct identification of the person concerned, to the statement of reasons and to any other data related thereto. As a reminder, Article 17, §3 of Regulation (EU) 2018/1725 provides that the right of access entails the right to obtain a copy of the personal data undergoing processing. Certainly, that right may not adversely affect the rights and freedoms of others; nonetheless, "the result of such considerations should not be a refusal to provide all information to the data subject".

Of course, in the fields of judicial cooperation in criminal matters and of police cooperation, Article 81, §1 of the Regulation provides that "the controller may restrict, wholly or partly, the data subject's right of access to

the extent that, and for as long as, such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to, [inter alia] protect the national security of Member States". In such cases, the controller must inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction. Nevertheless, such information may be omitted where the provision thereof would undermine, for example, national security. In addition, the controller must inform the data subject of the possibility of lodging a complaint with the European Data Protection Supervisor (EDPS) or of seeking a judicial remedy before the Court of Justice. Finally, the controller must also document the factual or legal reasons on which the decision is based and make available that information to the EDPS on request.

However, in the context of the CFSP, the above-mentioned limitations may not be invoked by the data controller. In that area, the right of access is "direct", in the sense that access can be obtained directly from the controller by the data subject and not through the EDPS. Consequently, the recent Council's Decision is accompanied by a data protection notice for the attention of the data subjects to whom the restrictive measures apply. According to that notice, the controller of the personal data processing operation is the General Secretariat of the Council which has appointed a Data Protection Officer (DPO) who can be contacted by data subjects for the exercise of their rights such as the right of access, as well as the rights to rectification or to object.

What is more, in the CFSP area, the right to receive a copy of the personal data undergoing processing may only be restricted by a legal act, in accordance with Article 25 of Regulation (EU) 2018/1725. To our knowledge, such legal act was not adopted yet. Under the regime of the Regulation's predecessor, Article 24 of the implementing measures contained in Council Decision 2004/644/EC foresaw that for legitimate reasons, such as national security, the controller could restrict the extent of the information to which the data subject might have access to. In that event, "except in case of absolute necessity, the controller shall first consult the DPO, whose opinion shall not bind the Institution. The controller shall reply to requests relating to the application of exceptions or restrictions to the exercise of rights without delay and shall substantiate this decision". Even though Decision 2004/644/EC still appears to be in force on Eur-lex, it seems doubtful to us that such an exception to a data subject's right could be considered compliant with Article 25, §2 of the "new" Regulation according to which the legal restricting act must contain specific provisions as to, inter alia, the purposes of the processing or categories of processing, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer and the risks to the rights and freedoms of data subjects.

In the context of restrictive measures, from the data subjects' perspective, the possibility to directly have access to unrestricted information processed by the Council – including data necessary for the correct identification of the person concerned by those measures as well as the statement of reasons explaining the reasoning of his/her inclusion into the list – obviously is an interesting additional means to secure their defense rights. Should they

not agree with the DPO's reaction, it goes without saying that, without prejudice to any judicial, administrative or non-judicial remedy, data subjects may lodge a complaint with the EDPS.