Octopus Virtual Conference on Cybercrime: forward-looking "outlook" session on human rights and the rule of law in cyberspace

18 November 2021

Robert Spano

President of the European Court of Human Rights

Dear Octopus participants,

Your conference has been going strong since 2007 and I have been pleased to participate in previous editions in 2016 and 2018. However , this is my first presentation as President of the European Court of Human Rights and I am honoured to represent the Court today.

Let me congratulate the Budapest Convention on its 20th anniversary. We can say that in 2001 the Budapest Convention was a real precursor in underlining the impact which the digital revolution would have on society, and in particular on the future of telecommunications, as well as anticipating the emergence of new types of crimes. The Budapest Convention has not stayed still but has also adapted to emerging challenges during the last two decades, through the First Additional Protocol, and now the Second Additional Protocol, which is expected to be open for signature next year.

Another crucial feature of the Convention and key to its success, is its truly global reach, which is reflected in the conference and the array of participants from around the world. Cyberspace itself is free of borders and your global approach, insisting on close and continuous cooperation between States, is evidently the correct one.

As my starting point, I think it is uncontroversial to state that the threats being faced by Contracting States and their citizens have proliferated in recent years[1], these include global terrorism, drug trafficking, human trafficking, and the sexual exploitation of children. Cyberspace and cyber-criminality has perhaps accentuated these phenomena.

On the other hand, the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information. The Internet provides essential tools for participation in activities and discussions concerning political issues and issues of general interest, it enhances the public's access to news and facilitates the dissemination of information in general.

The focus of this session is human rights and the rule of law in cyberspace. A careful balancing is required between for example, granting freedom of expression and moderating harmful or illegal content, or prosecuting cybercriminals while respecting rule of law guarantees. This balancing of rights is not something new to the Court, as I will demonstrate.

[1] *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, § 323, 25 May 2021

In my short presentation I will firstly provide a brief *tour d'horizon* of the types of cases which have come before the Strasbourg Court under the theme of cybercrime; secondly I will look at the positive obligations doctrine in this field; and thirdly address the rule of law safeguards that any criminal justice response must provide.

I. Cybercrime cases before the European Court of Human Rights

Cybercrime cases come to Strasbourg in all shapes and sizes, relying on a variety of Articles of the Convention (fair trial guarantees, right to respect for private life, freedom of expression and anti-discrimination provisions) and touching upon hate speech, child pornography and the dissemination of confidential information. Whilst we do not yet have a vast stock of cases, we are slowly building up clear jurisprudence. Let me give you three examples.

In *K.U. v Finland* from 2008 an unknown individual posted an advertisement of a sexual nature on an Internet dating site in the name of the applicant, who was twelve years old boy, which made him a target for approaches by paedophiles.[2]

[2] *K.U. v. Finland*, no. 2872/02, ECHR 2008

The applicant complained under Article 8 of the Convention that an invasion of his private life had taken place and that no effective remedy existed to reveal the identity of the person who had put a defamatory advertisement on the Internet in his name, contrary to Article 13 of the Convention.

In *Savva Terentyev v Russia*[3] from 2018 the applicant, a young blogger, was convicted for inciting hatred after posting remarks about police officers in a comment under a blog post. The Court found a violation of Article 10 because although the applicant's language had been offensive and shocking, that alone was not enough to justify the interference with his right to freedom of expression.

In *Beizaras and Levickas v Lithuania*[4] from 2020 hate-speech comments were left under a Facebook post which depicted two men kissing. The men asked the authorities to conduct a criminal investigation which they refused to do. The applicants complained that they had been discriminated against on account of their status, which had been the reason underlying the domestic authorities' refusal to open a pre-trial investigation.

[3] *Savva Terentyev v. Russia*, no. 10692/09, 28 August 2018
[4] *Beizaras and Levickas v. Lithuania*, no. 41288/15, 14 January 2020

The Court found a violation of Article 14 of the Convention, taken in conjunction with Article 8 as well as a violation of Article 13 (right to an effective remedy). In particular, the Court found that the applicants' sexual orientation had played a role in the way that they had been treated by the authorities, which had quite clearly expressed disapproval of them. Such a discriminatory attitude had meant that the applicants had not been protected, as was their right under the criminal law, from undisguised calls for an attack on their physical and mental integrity.

II. Positive obligations in the field of cybercrime

Now let me turn to the Contracting States' positive obligation to secure the effective enjoyment of the rights and freedoms under the Convention.

These obligations have already been elaborated by the Court under a number of Articles of the Convention and in cases which do not concern cyberspace[5], and the Court has no problem in applying them equally to cybercrime complaints.

[5] *Dink v. Turkey*, nos. 2668/07 and 4 others, §137, 14 September 2010

Let me give you an example. It is taken from the recent case of *Khadija Ismayilova v Azerbaijan*[6] from 2019. In that case, the applicant journalist received a threatening letter demanding her to cease her journalistic activities. Hidden cameras had been installed in her flat by unknown persons without her knowledge and consent, and intimate videos of her were taken secretly and disseminated on the Internet. She complained that her rights under Articles 8 and 10 had been breached, owing to the authorities' failure to protect her from unjustified intrusions into her private life linked to her work as a journalist.

The Court decided to approach the privacy complaint under Article 8 from the standpoint of the positive obligation on the State to investigate criminal offences against journalists. Having regard to the significant flaws in the manner in which the authorities investigated her case, as well as the overall length of the proceedings, the Court found under Article 8 that the authorities failed to comply with their positive obligation to ensure the adequate protection of her private life by carrying out an effective criminal investigation.

[6] *Khadija Ismayilova v. Azerbaijan*, nos. 65286/13 and 57270/14, 10 January 2019

As to her freedom of expression complaint under Article 10, the Court, in finding a violation, also approached this from the angle of the positive obligation which "*require(s) States to create, while establishing an effective system of protection of journalists, a favourable environment for participation in public debate by all the persons concerned, enabling them to express their opinions and ideas without fear, even if they run counter to those defended by the official authorities or by a significant part of public opinion, or even irritating or shocking to the latter*"[7].

III. Rule of law safeguards

Finally, I come to the third part of my intervention on safeguards. State actions in prosecuting cybercrime must respect rule of law guarantees.

In *Trabajo Rueda v Spain*[8] from 2017 the Court found a violation of the applicant's right to privacy where police seized and inspected his computer without prior judicial authorisation. The Court deemed that the interference had not been proportionate to the legitimate aims pursued and had not been "necessary in a democratic society" because there was no urgency for police to seize his computer and access his files without prior judicial authorisation.

[7] § 158.
[8] *Trabajo Rueda v. Spain*, no. 32600/12, 30 May 2017

Similarly, in *Benedik v. Slovenia* from 2018, the Slovenian police's failure to obtain a court order to access information associated with a dynamic IP (Internet Protocol) address constituted a violation of his right to privacy.[9] The law on which the contested measure was based and the way it had been applied by the domestic courts lacked clarity and did not offer sufficient safeguards against arbitrary interference. The interference with the applicant's right to respect for his private life was thus not "in accordance with the law".

The final case I wish to refer to concerns the blocking of websites. The legal framework in place must establish safeguards capable of protecting individuals from excessive and arbitrary effects of blocking measures. That was the conclusion of the Court in the case *of Vladimir Kharitonov v Russia*[10] from 2020, which found a violation of Articles 10 and 13 of the Convention.

[9] *Benedik v. Slovenia*, no. 62357/14, 24 April 2018
[10] *Vladimir Kharitonov v. Russia*, no. 10795/14, § ..., 23 June 2020

Let me conclude by saying that States have the not so easy task of fighting cybercrime in an effective and deterrent way on the one hand and on the other respecting rule of law safeguards of those, maybe the cybercriminals themselves, whose rights will necessarily be interfered with. This balancing act may not be a simple one, but it is essential both in cyberspace and as in the "real" world.

Thank you for your attention.