

## WEBINAR

### Cybersecurity and Human Rights

<b>Date and hour</b>	<b>17 December 2020</b> 15h00-17h00 CET
<b>Speakers</b>	<ul style="list-style-type: none"><li>— <b>Katrin NYMAN METCALF</b>, Cybersecurity East Project expert, Estonia</li><li>— <b>Marko Juric</b>, Deputy Dean Law Faculty, Zagreb University, Croatia</li><li>— <b>Eve Hunter</b>, Cybersecurity East Project expert, Germany</li></ul>
<b>Objectives</b>	<p>The purpose of the webinar is to provide a practical and down-to-earth discussion about the current state of human rights safeguards and guarantees applicable to state policies, regulations and measures to ensure security of cyberspace, against the background of COVID-19 pandemic.</p> <p>The webinar is intended to focus on the following aspects of cybersecurity and human rights:</p> <ul style="list-style-type: none"><li>- How cybersecurity policies and their application can protect rights and fundamental freedoms;</li><li>- How cybersecurity policies and their application can negatively affect rights and fundamental freedoms;</li><li>- Similarities between cybersecurity and cybercrime measures in protecting human rights and freedoms;</li><li>- The ways in which COVID-19 pandemic affected the balance and status quo regarding the subject matter.</li></ul> <p>The webinar is designed to encourage an interactive participation and to facilitate information sharing among participants, discussing relevant experiences, good practices, challenges, and opportunities.</p>
<b>Expected outcomes</b>	<ul style="list-style-type: none"><li>• Identify key rights of individuals and fundamental freedoms affected by cybersecurity policies and their application, in view also of the COVID-19 pandemic;</li><li>• Identify rights and freedoms that cybersecurity strives to enforce and protect, including positive obligation of states to ensure security, and how this is relevant in COVID-19 circumstances;</li><li>• Explore links between cybersecurity and cybercrime measures in human rights context.</li></ul>
<b>Participants</b>	<p>Up to 200 participants are expected.</p> <p>Each registered participant will receive a confirmation email one day prior to the webinar with instructions on how to connect and rules of engagement.</p> <p>The webinar will be held in English and no interpretation will be provided.</p>

<p><b>Background</b></p>	<p>Since onset of the COVID-19 global pandemic, majority of affected societies had to adjust to living and working online, safe, thus making free and uninterrupted access to information and communication technology more important than ever before. Naturally, this shift has brought questions and concerns related but not limited to privacy and security of such communications.</p> <p>While there is fairly limited but nevertheless growing body of regulation, research and case law concerning human rights safeguards and guarantees applicable to fight against cybercrime and use of electronic evidence in criminal cases – due to cybercrime being a criminal justice matter in the first place - cybersecurity and relevant human rights guarantees remain an area less addressed and discussed in balanced manner. Too often, the debate on the subject matter is bringing together highly polarising views along the lines of “security versus freedom” rather than seeking balance in recognizing potential positive and negative effects of strengthening cybersecurity for individual rights and freedoms.</p> <p>The current Webinar is thus an opportunity to look beyond more established subjects of criminal justice response and related human rights safeguards, by focusing on rapidly developing area of cybersecurity regulations and compliance, and to evaluate the rights and freedoms at stake that could be both protected and/or affected by cybersecurity measures. However, finding possible common ground on the subject matter between cybercrime and cybersecurity domains is equally important.</p> <p>Viewed from this perspective, the COVID-19 pandemic has not brought along particularly new questions, but rather amplified both positive and negative aspects of interaction between cybersecurity/cybercrime and applicable human rights. Finding appropriate balance in this new reality is an ever-shifting but nevertheless still important goal.</p>
<p><b>Expected duration</b></p>	<p>2 hours (1h for presentations, 1h for open discussion)</p>
<p><b>Relevant resources</b></p>	<p>European Union, <a href="#">Directive on security of network and information systems - NIS Directive</a> (2016)</p> <p><a href="#">Budapest Convention on Cybercrime</a>, especially Article 15</p> <p>European Union Agency for Fundamental Rights (FRA), <a href="#">Handbook on European law relating to cybercrime and fundamental rights</a> (2017)</p> <p>Council of Europe, <a href="#">Cybercrime and COVID-19 resources page</a></p>
<p><b>Related activities</b></p>	<p>The webinar is carried out under Outputs 1.3 and 2.2 of the CyberEast project, aiming at reinforcement of Article 15 of the Budapest Convention as well as improvement of interagency cooperation (Activity codes 1.3.2 2.2.2, PMM 92163).</p>