ERA Forum (2017) 18:291–296
DOI 10.1007/s12027-017-0468-1

EDITORIAL

Updating and diversifying the training offer for EU legal practitioners to meet the challenges posed by the new technologies

Laviero Buono[1]

EUROPÄISCHE RECHTSAKADEMIE
ACADEMY OF EUROPEAN LAW
ACADEMIE DE DROIT EUROPEEN
ACCADEMIA DI DIRITTO EUROPEO
TRIER · TREVES · TREVIRI

Published online: 6 July 2017

The impact of new technologies in criminal proceedings

Nowadays, legal practitioners have to face new challenges to keep up with the continuous high-speed evolution of technology. These challenges are posed by cloud computing (not knowing where data is stored in the world), by encrypted digital files (which can hardly be opened with brute force) by proxy servers (that facilitate anonymity online) by jurisdictional issues (not knowing which court is competent). It is therefore crucial for them to take up these challenges, to start becoming familiar with all the above-mentioned issues and to share experiences on similar internet-related criminal cases with their peers within and outside Europe.

The massive use of internet, social networks and digital media have favoured criminal practices. Traditional types of fraud and crimes have been modified to use new tech channels. In almost all judicial proceedings, information gathered from the internet plays a significant role and is due to become even more important in legal practitioners' operational work. For them the web has become a vital tool as browsers, search engines and social media monitoring tools can assist in the retrieval of the information needed. Almost all criminal courts are confronted for example with the question of whether electronic evidence presented in criminal proceedings are admissible or not. Challenges governing the authenticity of electronic data vary in the legal framework of different Member States and are continuously challenged by the evolution of technological devices. An example of the types of digital devices encountered by a digital forensic practitioner includes not only computers and laptops but also

✉ L. Buono
lbuono@era.int

[1] Academy of European Law (ERA), Metzer Allee 4, 54295 Trier, Germany

USB thumb drives, mobile (smart) phones, digital cameras, satellite navigation systems and much more.

Several recent policy documents of the European Union (EU) recognised that for legal practitioners such as judges, prosecutors and defence lawyers, practical and legal obstacles continue to exist, mainly due to the rapid development of technologies, e.g. in cases where the origin of online crime or location of the digital evidence is not (yet) known or volatile, or in cases where conflicting regulations hamper the cooperation with service providers.

Back in April 2015, the EU in its Communication: "EU Agenda on Security" noted that: "*Cyber criminality requires competent judicial authorities to rethink the way they cooperate within their jurisdiction and applicable law to ensure swifter cross-border access to evidence and information, taking into account current and future technological developments such as cloud computing and Internet of Things. Gathering electronic evidence in real time from other jurisdictions on issues like owners of IP addresses or other e-evidence, and ensuring its admissibility in court, are key issues".*[1]

In October 2016 the European Cybercrime Centre (EC3) within Europol issued the "Internet Organised Crime Threat Assessment (IOCTA) 2016" which reads: "*Law enforcement must continue to develop and invest in the appropriate specialised training required to effectively investigate highly technical cyber-attacks. A foundation level understanding, including the basics of digital forensics* (*e.g. how to secure/seize digital evidence*) *should be required by all law enforcement officers".*[2]

Finally, in June 2016, the Council of the EU adopted the "Conclusions on improving criminal justice in cyberspace". Three main points were adequately stressed: (a) cooperation with service providers is to be enhanced, (b) mutual legal assistance (MLA) proceedings (and where applicable, mutual recognition) need to be streamlined and (c) rules on enforcement jurisdiction in cyberspace should be reviewed.[3]

Cooperation with the private sector is vital in effectively conducting online investigations. Not only does the private sector hold much of the critical evidence, but private party takedowns of criminal infrastructures, removal of illicit content and reporting of data breaches to law enforcement are among the most effective measures to stop internet-related crimes. For EU judges, prosecutors, defence lawyers, it is vital to "physically" meet representatives of the internet industry, to debate issues in the framework of training activities, to listen to their presentations and to ultimately stay in touch with them. On MLA instruments, there is little doubt that these instruments were not conceived for the digital age. Legal proceedings, in particular international requests of mutual assistance, are slow and often with uncertain results. This regrettable status quo causes significant delays in international criminal investigations, especially when data is per se volatile such as an IP address which can be

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—The European Agenda on Security, Strasbourg, 28.4.2015, COM(2015) 185 final.

[2] Europol: "Internet Organised Crime Threat Assessment (IOCTA) 2016", p. 13. The full report is available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

[3] Council of the European Union, Conclusions on Improving Criminal Justice in Cyberspace, Luxembourg, 9.6.2016.

moved within seconds. The need to shorten time limits for replying to international requests of mutual legal assistance in internet-related cases is a *condition sine qua non* to effectively tackle these crimes.

ERA training events on cyber-related issues and e-evidence 2012–2017 and beyond...

Against the background of the ever-increasing number of challenges related to the impact of Information and Communication Technologies (ICTs) in criminal procedures, ERA's training offer has not only been regularly updated over the past few years, but also considerably diversified. Besides the reputation ERA had previously gained at EU level in the fields of criminal justice and judicial cooperation in criminal matters, ERA has consistently increased its profile in further fields of expertise, such as cybercrime, electronic evidence and the overall impact of new technologies in criminal proceedings (online investigations, internet searches, etc.). On these topics ERA implemented several projects co-financed by the European Commission under the Criminal Justice, ISEC and Justice Programmes. All projects consisted of series of seminars implemented in various EU cities. They were all intended as platforms to demonstrate how ever more frequently ICTs are impacting on legal and judicial proceedings.

Below a selection of the major projects co-financed by the European Commission and implemented by ERA in the past five years.

- 2012–2015/Fighting the illegal use of the internet—series of six intensive seminars for 300 EU legal practitioners (HOME/2011/ISEC/AG/INT/4000002230)

This project consisted of six seminars implemented in Madrid, Lisbon, Vilnius, London, Sofia and Stockholm. All seminars were intended as a platform to debate and assess how European legislation in the field of cybercrime is applied in the different Member States and Candidate Countries and the perspectives for an effective Europe-wide campaign against illegal use of the internet. Each event offered a mixture of training methods, varying from introductory and more in-depth lectures to case studies and other types of interactive learning. Particular attention was given to discussion in small working groups. Lectures and workshop sessions were presented by EU and national experts.

- 2012–2015/Training Centre on Cybercrime for judges and prosecutors (HOME/2011/ISEC/AG/INT/4000002194)

This project consisted of eight seminars that took place in Trier, in Germany. It comprised basic training courses on the legal and technical aspects of cybercrime to provide some 500 judges and prosecutors with the essential skills necessary to cope with internet-related offenses.

All events enabled participants to gain an overview of EU policy on internet-related offences and familiarise them with the current work being carried out by the EU and other European and international institutions and organisations. Real-life cybercrime scenarios were discussed in small working groups.

- 2013–2014/The impact of internet, new technologies and social networks on EU criminal justice (JUST/2011/JPEN/AG/2879)

All in all, three seminars, one of introductory nature: "An introduction to electronic evidence as a new category of evidence: examples and related practical challenges, legal considerations and need for harmonisation" and two specialised: "Challenges in obtaining and relying on electronic evidence from overseas (Hotmail, Gmail, Yahoo!, Facebook and others) and issues of admissibility in Court—a comparative analysis of the common and continental law approaches" and "The admissibility of electronic evidence when cybercrimes are committed (identity theft, child pornography, on-line fraud cases, etc.)"

- 2014–2105/The admissibility of electronic evidence (e-evidence) in criminal proceedings (JUST/2013/JPEN/AG/4481)

The general objectives of this series of three events implemented in Lisbon, Riga and Bucharest was to debate, assess and scrutinise the validity and admissibility of electronic evidence in criminal proceedings. Each seminar had a specific focus: (a) fundamentals of electronic evidence and its practical foundations illustrated with relevant case law, (b) planning and justifying the search and seizure of electronic evidence in criminal proceedings before presenting it to court and (c) specific legal and technical considerations for all players in the criminal justice system in handling electronic evidence.

- 2015–2017/Investigating, prosecuting and adjudicating criminal cases in the online world: challenges (and opportunities) posed by the Internet to EU legal practitioners (JUST/2014/JTRA/AG/EJTR/6772)

Main aim of this series of five events (held in Budapest, Madrid, Lisbon, Cracow and Trier) was to provide legal practitioners with the basic understanding of the internet architecture and concepts (Internet Protocol, anonymity online, encryption, cloud computing, etc.) enabling them to gain an overview of the challenges related to the conduction of online investigations. All events also offered an insight into the work carried out by their counterparts in other Member States on these new investigative techniques, developing mutual trust among Member States while expanding good practices

- 2016–2017/The life cycle of the electronic evidence in criminal proceedings (JUST/2015/JTRA/AG/EJTR/8650)

This Project consisted of six events (implemented in Zagreb, Madrid, Athens, Trier, Prague and Tallinn) which aimed at presenting the whole life cycle of the electronic evidence from the pre-trial to post-trial phase. Participants, through a practice-oriented methodology made up of concrete simulations and live demonstrations, learnt the basics of digital investigations.

Besides the co-financed series of seminars, ERA organised also several cyber-related open events across Europe. Worth mentioning is the first edition of the "Cybercrime Mock Trial" (Trier, 25–26 April 2016). The Mock Trial attended by quotas of judges (6), prosecutors (11) and defence lawyers (9), was a practice-oriented exercise of a legal procedure that was the actual enactment of a fictitious cybercrime case. Participation in the trial provided the participants with an insider's perspective from which to learn about the application of substantive and procedural cybercrime rules. The course helped participants in gaining a basic understanding of the legal mechanism through which a hypothetical cybercrime dispute could be conducted in trial regardless of the concrete national procedural setting. Moreover, it helped them develop critical thinking skills, oral skills, understanding of substantive/procedural areas of law and international cooperation rules.

Admission to the course was limited to 25 participants (including a quota of 9 defence lawyers for the "defence" team), to maximise interaction and one-to-one contact with experts and trainers. The whole course was conducted through a "learning-by-doing style" encouraging group discussions and sharing of experiences. The goal was to create a natural realistic court situation with the defence team, the prosecution team and the judges (assisted by the "assessor judges") who carefully steered the discussion.

Adapting the training offer to meet the challenges posed by the new technologies

Though the use of ICTs, potentially, almost all forms of "traditional" crimes can be committed via internet in the future. This is the case as regards the recruitment and training of terrorists, illegal drug smuggling, illegal online gambling, fraud committed using cloned credit cards, the trade of sexual images of children. Therefore, whatever the specialisation of the judges and prosecutors is (whether it be investigations in the financial and banking sector, or in the telecommunications area, the fight against organised crime and terrorism, the sexual exploitation of children, etc.) future well coordinated training schemes are needed to provide to the largest possible number of EU legal practitioners the basic skills necessary to understand the internet architecture: Internet Protocols, anonymity online, proxy servers, encryption, internet cache, VoIP, etc.

Such training events shall be conducted in a "learning-by-doing" style which, through demos and simulations, encourages participants to use their own laptops/pads and follow the exercises (open source tools, geo-location software, anonymity online, etc.). The methodological approach shall be based more on simulations, role playing and live demonstrations rather than theoretical talks. Such live demonstrations will show the technical and legal problems that judges, prosecutors and lawyers are confronted with in handling online cases. Changes will be tangible because at the end of the training participants will go home not with a "theoretical" knowledge, but with a practical lesson learnt on how colleagues are dealing (or have dealt) with similar internet-related cases. Through live demonstrations, using internet open source tools, it will be shown to participants how forensically complicated it is to extract evidence from mobile devices, how criminals can hide behind fake servers when committing online fraud, how paedophiles (mis)use chatrooms to groom children. All programmes shall be constructed in an interactive, practice-oriented way and will ultimately assess how the internet searches' results can be presented, based on their authenticity, in court.

Finally, there is an increasing need to talk with the private sector (public/private partnership) and the internet industry. If potentially, as explained above, all crimes can be committed with the use of internet, then bilateral cooperation between judges and between prosecutors (also from different countries) is insufficient. High-tech crimes cannot be adequately investigated, prosecuted and adjudicated upon without cooperation with industry. Dialogue with internet service providers such as Google, AOL, Microsoft, Skype, Facebook, eBay, Visa, Mastercard and many others will be key for judges and prosecutors to prevent, detect and respond to crimes committed using information and communication technologies facilities. It is therefore crucial to initiate such public-private dialogue in the framework of training activities.