Searching for crime on the web: Legal and Ethical perspectives

Authors:
Dimitrios Kavalleros, Christina Chalanouli, Georgios Kokkinis, Georgios Leventakis, Anastasios Papathanasiou, Efthimios Lissaris, Georgios Giataganas, Georgios Germanos
Questions of interest

➢ Under which conditions is an investigation authorised/permitted?
➢ Which are the legal boundaries and the applicable operational rules?
➢ Is the Data Protection Regulatory framework respected?
➢ Does the MS legislation permit the use of the same platform/toolkit to fight against serious and organised crime?
➢ Is it possible to regulate the Dark Web?
• Complex legal framework
  • National
  • European
  • International
• Technology advances rapidly
  • Organised crime
  • Terrorist groups
• Law Enforcement – Daily Activities
Legal and Ethical Challenges

- General Data Protection Regulation (GDPR) 679/2016
- Directive 680/2016 on the protection of natural persons with regard to the processing of personal data by competent authorities
- NIS Directive
- United Nations Global Counter-Terrorism Strategy
- European Convention for the Protection of Human Rights and Fundamental Freedoms
- Directive 2013/40/EU on attacks against information systems
- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
### Legal and Ethical Challenges

<table>
<thead>
<tr>
<th></th>
<th>GREECE</th>
<th>SPAIN</th>
<th>GERMANY</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data protection as an absolute restriction</td>
<td>Not when reasons of national security are met or serious crimes are committed, based on Law 2225/1994 &amp; Law 2472/1997.</td>
<td>Spanish Organic Law 35/1999 on personal data and Royal Decree 1720/2007. Not applicable to the processing of files related to the investigation of terrorism and serious forms of organized crime, or the investigation of other serious criminal offences.</td>
<td>Based on Articles 1,2,10,13 of German Constitution Article 13 BDSG (Federal Data Protection Act): Infringements of this right is possible within narrow boundaries. Preventive state interventions – especially in the framework of online searches – are only permissible constitutionally, if factual indications exist of a concrete danger to a predominantly important legal interest.</td>
<td>Data Protection Act 1998 (DPA). The critical issues in the fight against terrorism are the conditions under DPA in which police officers would be privileged to breach data protection laws which fall under the implementation of EU Directive on Combating Terrorism.</td>
</tr>
<tr>
<td>Search robots</td>
<td>This is not provided by law.</td>
<td>This is not provided by law. Nevertheless, based on Article 588 of Spanish Criminal Procedure Law. OSINT gathering is permitted without judicial authorization. For other types of information, legal consideration is necessary.</td>
<td>This is not provided by law.</td>
<td>Based on Section 48-RIPA and the Investigatory Powers Act 20001, public authorities can use online research and investigation tools but they must ensure that any interference with a person's right to respect for their private and family life is necessary for a specific and legitimate objective.</td>
</tr>
<tr>
<td>Agent provocateur</td>
<td>Illegal practice, based on Article 46 of Greek Penal Code.</td>
<td>Illegal practice based on Article 282 Spanish Criminal Procedure Law.</td>
<td>If a person has committed a crime, even because he was encouraged by a LEA, the responding Federal State will conduct a criminal proceeding. However, the act of encouraging an individual to commit a crime violates the basic principle of fair proceedings and will lead to a procedural impediment based on Article 26 StGB (German Penal Code).</td>
<td>Based on Section 26-RIPA, English law offers someone accused of a crime a defence if they can show an officer acted as an agent provocateur, meaning they initiated or instigated the crime.</td>
</tr>
<tr>
<td>Acceptance of data gathered in court</td>
<td>Only data gathered in compliance with Law 3917/2011 &amp; Law 3115/2003.</td>
<td>The Criminal Procedure Law (Articles 588 &amp; 589) introduces provisions concerning the retention of data and other information contained in computers or other electronic devices in order to preserve the integrity and the eligibility of these materials in court proceedings.</td>
<td>Based on Article 104 of The German Criminal Procedure Code &amp; Article 110A, evidence has to be seized and secured according to law requirements. In some case, accidentally or illegally obtained information may be accepted. Lawful interception regulates the monitoring of telecommunication activities and content.</td>
<td>According to the 4 basic Principles of Good Practice Guide for Digital Evidence, a national best practice guide produced by ACPO -2007.</td>
</tr>
</tbody>
</table>
Technological Challenges

• Dark Web
  • High level of anonymity
  • Multiple darknets – employment of different technology (e.g. TOR, I2P, )

• Dark markets (e.g. malware, hacking toolkits, 0day vulnerabilities, hacking as a service etc.)
  • High volume
  • A lot of time is needed for covert operation

• Cryptocurrencies
  • Increased anonymity
  • Difficult to trace the “money route”
LEAs facing **multidisciplinary** challenges:

- Evolving criminal landscape
- Identification of illegal activities
- Identify the physical location of the machine(s) hosting the website/service
- Multiple jurisdictions
- Detect and apprehend the actors
- Time constrains

LEAs Cybercrime investigations **take place within a complex** framework of Legal and Ethical rules and **simultaneously follow up the technological advancement** of Cyber perpetrators
TENSOR aims at developing a platform that provides LEAs with tools necessary to enhance their capacity for dealing with huge amounts of online content in the early detection of online terrorist organised activities, radicalisation and recruitment.

It is expected that TENSOR tools will have a positive impact on LEAs’ ability to:

• Accurately identify terrorist online communities;
• Detect and prevent terrorist activities organised online;
• Identify novel terrorism trends;
• Detect mis-information, propaganda and recruitment materials;
• Gather and preserve data for forensic analysis;

• **Ensure compliance with National and EU regulations regarding data protection and LEA investigation**
TENSOR Crawler:
- Crawl the (Surface/Dark) Web by starting from a URL of interest
- Instead of traversing all links, select to follow only the ones relevant to your interests
- Hyperlink selection is based on machine learning approaches
- Increased efficiency and effectiveness

TENSOR Profiling Tool
- Accurate profiling
- Dialogue analysis and management
- Seven categories with 73.02% success
- 29.145 posts by 170 different authors – 78.44% success
➢ Economical impact of cyber crime activities
   ➢ Cyber security measures
   ➢ Mitigation actions
   ➢ Dark Web economy associated with cyber attacks (e.g. 0day Vulnerabilities and Hacking as a Service)

➢ Develop automated tools for information gathering (e.g. SNA)

➢ Develop an automated platform for behavioural, social and economic analysis of the cybersecurity risks and the cybercrime market.

➢ Provide a set of recommendations about the reduction of cybercrime to all relevant stakeholders including policy makers, regulators, law enforcement agencies, relevant market operators and insurance companies
SAINT Social Network Analyzer
European countries enacted legislation in accordance with the international and European regulatory framework.

However, the extent of internet along with the existence of grey areas, such as dark or/and deep web render web’s regulation an almost *mission legally impossible*.

We need to act proactively respecting legal and ethical principles in order to prevent e-illegal acts.

We need to prioritize areas and sectors and promote cooperation of different disciplines.
Thank you for your attention!

Research Associate
Tel.: +30 210 7481630 (ext.399)
e-mail:

project-saint.eu
www.kemea.gr
tensor-project.eu