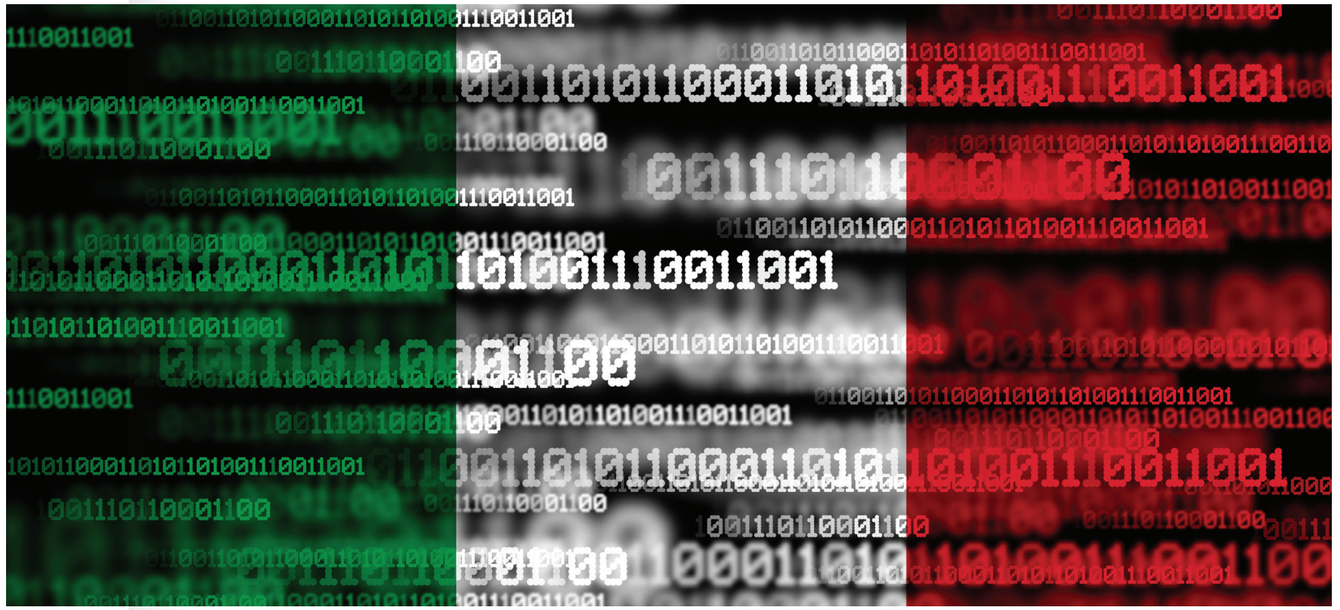
Thought Leader

The Threat of Cybercrime in Italy



As modern society becomes fully digitalised, cybercrime's potential to cause damage grows ever greater. This threat is especially magnified as digital attacks become a staple of warfare. In this feature, criminal lawyer Licia Dal Pozzo draws upon her experience in handling cybercrime cases to outline the threat cybercrime poses to Italy and the EU as a whole.

To begin with, what are the key Italian laws and statutes concerning cybercrime?

First of all, I point at the Criminal Code, which since 2008 has provided for and punished cybercrimes in the strict sense. These include cyber fraud, abusive access to a computerised or telematic system, damage to data and software, dissemination of viruses and malware, and other crimes that can also occur as cybercrime, such as extortion, identity theft, money laundering, misuse of payment cards, solicitation of minors, revenge porn, and cyberstalking. Equally relevant are special laws that punish additional crimes that can also be committed through the Internet, including intellectual property infringement.

In relation to the prosecution of cybercrime, relevant laws include L.L. 48/2008, which ratified the 2001 Council of Europe Cybercrime Convention, known as the Budapest Convention, and the law on the establishment of the European Investigation Order, which established international cooperation in the investigative field. Specific mention should be made of Decree Law 82/2021, which established the National Cybersecurity Agency, aimed at combating cybercrimes that harm national interests.

The relevant European regulations are many, and among them, I highlight Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems; the Digital Operational Resilience Act, which become effective as of 16 January 2023, in order to create a common framework for financial sector oversight; and Council Decision 2023/436 of February 14, 2023, authorising member states to ratify the Second Additional Protocol to the Convention on Cybercrime regarding enhanced cooperation and disclosure of electronic evidence to improve global cooperation among investigative forces and implement investigative tools.

STUDIO LEGALE DAL POZZO
DIRITTO PENALE

> ***"Today, cybercrime is mainly carried out by organised crime and foreign states, no longer just by individual offenders."***

What is the scale of the threat that cybercrime poses to Italian organizations?

Today, cybercrime is mainly carried out by organised crime and foreign states, no longer just by individual offenders.

The report 'Intellectual property crime threat assessment 2022' by EUIPO and Europol is interesting: it estimated that counterfeit and pirated goods worth €119 billion were imported into the EU in 2019, accounting for 5.8% of EU imports. It also estimated that over the period 2013-2017, lost sales due to counterfeiting amounted to more than €83 billion per year. This corresponds to estimated losses of €15 billion in tax revenue and 171,000 jobs in total. Intellectual property crimes cause damage to the reputations of legal producers while harming fair production and distorting market competition. In addition, intellectual property crimes reduce funds available for public research and innovation.

In your experience, what forms of cybercrime are most typically the subject of criminal charges?

They are electronic payment instrument scams, computer system hacking, sensitive data appropriation, and extortion or attempted extortion if the ransom is not paid.

In what ways does the prosecution of a cybercrime differ from other criminal cases?

The difference may be found in the complexity of computer evidence, as it has typical characteristics that distinguish it from other sources of evidence. These characteristics include:
- the promiscuity of data;
- the plurality of information contained in computer systems and

immateriality, with an attitude for rapid and easy circulation – it is difficult to limit the search to specific data and information;
- transnationality and delocalisation – digital data are often allocated on servers or devices located in countries other than those where investigations are carried out or on the cloud, meaning problems of international judicial cooperation and territorial jurisdiction may arise;
- the subject matter has a high specialised connotation and requires specific technical skills that not all investigating offices have, let alone most lawyers;
- there is a high danger of manipulation and alteration of evidentiary material;
- there is anonymity in operations;
- there is still no international authority on the subject that would facilitate investigations, but we trust that the Proposal of United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes may be realised.

In conclusion, one may understand that identifying the perpetrators of criminal acts is particularly arduous.

What changes have you observed in the climate of criminal law and cybercrime during your time in practice?

The technological development required by cybercrime punishment changed the process; today, cyber data has become the centre of it.

In its latest Annual Report, covering 2021 activities, Eurojust devotes a chapter to the fight against cybercrime in which it highlights how online criminal activities have increased in frequency, numbers and aggressiveness, and that Eurojust's main activities of intervention have been ransomware, artificial intelligence, cryptography and cybercrime as a service. The number of victims recorded on a daily basis is high.

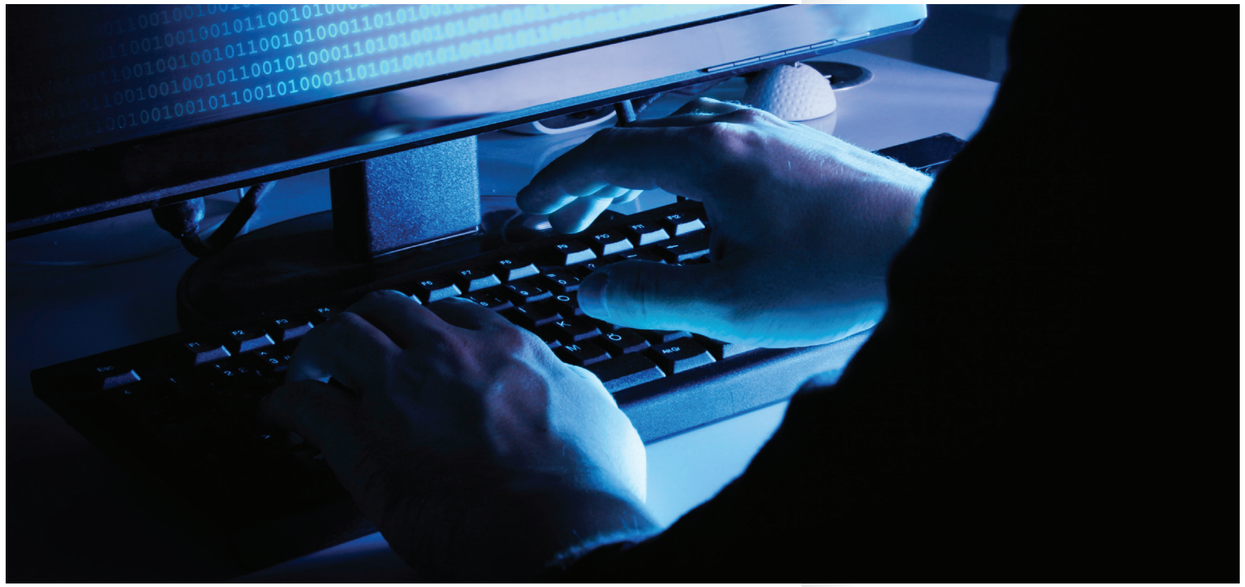
Do you have any projections for how cybercrime and laws surrounding it may change in years to come?

They say that artificial intelligence will be able to facilitate investigations by increasing the level of technological expertise needed and the ability to process cyber data. Change on the regulatory level must be rapid in order to catch up with the rapid development of cybercrime. In addition, action should also be taken on prevention that can be implemented by both companies and police, in terms of both human and technological resources.

What would your first piece of advice be for a firm that believes it has become, or is in danger of becoming, the victim of a ransomware attack?

Do not give in to the temptation to offer a ransom, because there is no guarantee of the restoration of systems and the return of stolen data. Instead, immediately seek the intervention of the Judicial Authority by filing a timely complaint with the help of a legal counsel. Any omitted report increases the vulnerability of the system, so reporting is not only in one's own interest but contributes to the collective good.

In perspective, it is advisable to adopt appropriate prevention systems that control the chain of suppliers, especially the smaller and more vulnerable ones, and to increase investment in digital security to acquire highly specialised labour resources and effective IT alerting systems.



> ***"The technological development required by cybercrime punishment changed the process; today, cyber data has become the centre of it."***

Do you have any further comments that you would like to add regarding cybercrime in your jurisdiction?

I will end with a mention of hybrid warfare, which is not only relevant to my jurisdiction but also to it. The term first appeared in 2006 in reference to the war in Lebanon. The technique progressed, for example with ISIS, and today it is recurring. The cyberattack strategy is one of the offensive means and represents the most damaging and broadest level of conduct that falls under cybercrime. The effects are highly damaging and effective for the attacker, but the tools of defence are not ready yet.

For example, in Italy, spear-phishing campaigns against local media and various organisations operating mostly in the IT, energy, finance and refugee assistance sectors were recorded in late 2022, according to a 2023 Microsoft report on techniques and tactics adopted by Russia against Ukraine and NATO countries.

International law is stuck with a classical notion of war, meant in the kinetic sense, which excludes any cyberattacks from the area of prohibition of the use of violence. First of all, it is necessary to develop amendments to the law, and it is also relevant that not only every state, but also both large and small companies, implement effective systems of resistance and resilience towards this type of aggression, which is increasingly frequent and very dangerous.

About Licia Dal Pozzo

Licia Dal Pozzo is an advocate based in Milan, Italy. Her speciality is in criminal law, with experience in handling a range of subject matters including cybercrime, IP enforcement, tax crimes and corporate crimes.

STUDIO LEGALE DAL POZZO
DIRITTO PENALE

Contact

Licia Dal Pozzo
Founder
Studio Legale Dal Pozzo
Viale Abruzzi, 7 - 20131 Milano MI, Italy
Tel: +39 02 2941 1289
Fax: +39 02 2040 2080
E: licia.dalpozzo@studiodalpozzo.net