

EFFECTIVE INVESTIGATION IN THE AGE OF DIGITALIZATION



INTERNATIONAL ASSOCIATION
OF PROSECUTORS 1ST PAN
EUROPEAN REGIONAL CONFERENCE

02-05 May 2023
İstanbul - Türkiye

TUESDAY, 2 MAY 2023

All day



Arrival and on-site registration of conference participants

Venue: CVK Park Bosphorus Hotel

20.00 – 22.00



Welcome Reception



Translation into Turkish, English, French

Venue: CVK Park Bosphorus Hotel

Dress code: Business Attire/National Dress

Master of Ceremony: **TBD**

Speakers:

- **Bekir Şahin**, General Prosecutor of the Supreme Court of Appeal of the Republic of Türkiye
- **Han Moraal**, Secretary-General of IAP

WEDNESDAY, 3 MAY 2023

09.30–11.00



Official Opening Ceremony



Translation Throughout the Conference into Turkish, English, French







Master of Ceremony: TBD






Tribute and Turkish National Anthem

Presentation of the General Prosecution Office of the Supreme Court of Appeal

Speakers:

1. **Bekir Şahin**, General Prosecutor of the Supreme Court of Appeal of the Republic of Türkiye
2. **Kamran Aliyev**, IAP Vice-President and Prosecutor General of the Republic of Azerbaijan
3. **Bekir Bozdağ**, Minister of Justice of the Republic of Türkiye (**TBC**)
4. **Mehmet Akarca**, President of the Supreme Court of Appeal of the Republic of Türkiye (**TBC**)

<p>11.00 – 11.45</p> 	<p>Family Photo and Refreshment Break Press Statement / Interviews</p>
<p>11.45–12.30</p> 	<p>Introduction to the IAP Projects and the Prosecutors International Cooperation Platform</p> <p>Master of Ceremony: TBD</p> <p>Speakers:</p> <ol style="list-style-type: none"> 1. Han Moraal, Secretary-General of IAP 2. Janne Holst Hübner, Executive Director 3. Shenaz Muzaffer, General Counsel
<p>12.30 – 13.30</p> 	<p>Lunch</p>
<p>13.30 – 15.00</p> 	<p>Plenary 1: Appearance and Effects of Digitalization in the Criminal Procedure</p> <p>1.1 Gathering and use of digital evidence in criminal procedure in the context of effective investigation</p> <p>1.2 Effects of Second Protocol of the Budapest Convention on economic crimes, (challenges and responds in 24/7 applications)</p> <p>1.3 Illegality problem in digital evidence</p> <p>Master of Ceremony TBD</p> <p>Chair: Ali AlBuainain, Attorney General, Bahrain</p> <p>Speakers:</p> <ul style="list-style-type: none"> • Fulvio Baldi, Deputy Prosecutor General, Prosecutor’s Office at Supreme Court, Italy • Ilgar Safarov, Senior Assistant to the Prosecutor General, General Prosecution Office, Azerbaijan • Jan Kerkhofs, Member of the Cyber Unit, Federal Public Prosecutor's Office, Belgium • Yves Nicolet, Federal Prosecutor, Head of Cybercrime Unit and Francesca Pedrazzi, Prosecutor Specialized in Cybercrime Matters, Office of Attorney General, Switzerland <p>Q&A</p> <p>Rapporteur: TBD</p>
<p>15.00-15.30</p> 	<p>Refreshment Break</p>
<p>15.30 – 17.00</p> 	<p>Plenary 2: Fighting Against Economic Crimes in the Age of Digitalization</p> <p>2.1 Investigation procedure of the crimes committed with crypto currencies</p> <p>2.2 Use of crypto currencies for money laundering/Its investigation methods</p> <p>Master of Ceremony TBD</p> <p>Chair: Kamran Aliyev, IAP Vice President, Prosecutor General, Azerbaijan</p>

	<p>Speakers:</p> <ul style="list-style-type: none"> • Mark Carroll, Director Criminal Justice, International Justice Development, United Kingdom • Nathan Brooks, US Department of Justice International Computer Hacking and Intellectual Property Attorney, USA Embassy in Romania, Romania • Thomas Goger, Senior Prosecutor/Permanent Head, Central Bavarian Cybercrime Division, Germany • Ursula Schmudermayer, Senior Public Prosecutor, Austrian Central Prosecution Authority for the Prosecution of Economic Crime and Corruption, Austria <p>Q&A</p> <p>Rapporteur: TBD</p>
17.00 – 17.15 	Closing of the day
17.15 – 18.30 	Free time
18.30–20.00 	<p>Dinner</p> <p>Venue: CVK Park Bosphorus Hotel Dress code: Business Attire/National Dress</p>
20.00 	Cultural Event (Oporet at the Atatürk Cultural Center)
THURSDAY, 4 MAY 2023	
09.30 – 11.00 	<p>Plenary 3: Artificial Intelligence in Criminal Procedure</p> <ul style="list-style-type: none"> 3.1 Country practices regarding artificial intelligence 3.2 Criminal liability of artificial intelligence 3.3 Results of use of artificial intelligence in criminal procedure <p>Master of Ceremony TBD Chair: TBD Speakers:</p> <ul style="list-style-type: none"> • Jacqueline Bonnes, Senior Public Prosecutor Cybercrime and Digital Evidence / Co-chair Global Anti-Fraud Enforcement Network, Central Public Prosecutor’s Office for Combatting Economic Crime and Corruption, Netherlands • Nicola Lettieri, Deputy Prosecutor General, Prosecutor’s Office at Supreme Court, Italy • Prof. Dr. Çetin Arslan, Head of Department of Criminal and Criminal Procedure Law, Professor of Criminal and Criminal Procedure Law, Academician/Lawyer, Hacettepe University, Türkiye

	<ul style="list-style-type: none"> TBD <p>Q&A</p> <p>Rapporteur: TBD</p>
11.00 – 11:30 	Refreshment Break
11.30 – 12:00 	<p>Keynote (closing speech) and closing of the conference</p> <p>Keynote speaker: TBD</p> <p>Speakers:</p> <ol style="list-style-type: none"> Han Moraal, Secretary-General of IAP Kamran Aliyev, IAP Vice-President and Prosecutor General of the Republic of Azerbaijan Bekir Şahin, General Prosecutor of the Supreme Court of Appeal of the Republic of Türkiye
12.30 – 14.00	Lunch Break and Registration of local prosecutors attending training session
14.00 – 15.00 	<p>Introduction to the IAP Standards and Kick-Start of Training Session (for local prosecutors, also accessible for participants)</p> <p>Venue: İstanbul Çağlayan Court House</p> <p>Trainer: Shenaz Muzaffer, IAP General Counsel</p>
15.00 – 16.00 	<p>Training Workshop 1: Ensuring Fairness in the Criminal Justice Process</p> <p>Trainer: Vasily Lukashovich, Senior Lawyer, European Court of Human Rights</p>
16.00 – 16.30	Refreshment Break/PICP and GTA Lounge
16.30 – 17.30 	<p>Training Workshop 2: Ensuring Fairness in the Criminal Justice Process</p> <p>Trainer: Holly Scott-Mason, Liaison Prosecutor, Crown Prosecution Service, British Embassy Ankara</p>
17.30 – 18.00 	Closing of Training Session
14.00 – 19.00 	<p>Social Program:</p> <p>Tour in Historical Peninsula:</p> <ul style="list-style-type: none"> -Topkapı Palace -Hagia Sophia Mosque -Basilica Cistern -Bosphorus Tour
19.30 – 22.00 	<p>Farewell Dinner</p> <p>Venue: Çırağan Palace</p> <p>Master of Ceremony: TBD</p> <p>Speakers: Bekir Şahin, General Prosecutor of the Supreme Court of Appeal of the Republic of Türkiye</p> <p>Dress code: Smart Casual</p>

22:00- 22:30 	Return transfer to the hotels
FRIDAY, 5 MAY 2023	
All day	Airport Transfers – Participants of the Regional Conference

Al Sig. Procuratore generale

Pres. Luigi Salvato

Al Sig. Avvocato generale

Pres. Renato Finocchi Ghersi

Sede

I sottoscritti, dottori Nicola Lettieri e Fulvio Baldi, avendo partecipato alla Conferenza Regionale Paneuropea dell'Associazione internazionale dei Pubblici Ministeri (IAP) tenutasi ad Istanbul dal 2 al 5 maggio 2023, portano a conoscenza delle SS.LL. quanto segue.

Alla conferenza hanno partecipato, oltre al Paese ospitante ed alla delegazione italiana, le delegazioni di Austria, Azerbaijan, Bahrain, Belgio, Bosnia – Erzegovina, Bulgaria, Congo, Danimarca, Estonia, Finlandia, Georgia, Germania, Kazakistan, Corea del Sud, Marocco, Olanda, Pakistan, Filippine, Portogallo, Sud Arabia, Scozia, Sudan, Svizzera, Tagikistan, Tanzania, Thailandia, Regno Unito, Stati Uniti d'America.

I lavori si sono svolti nell'arco di tre giorni. Dopo le introduzioni di rito della prima giornata, la prima sessione si è soffermata sugli effetti della digitalizzazione nella procedura penale, la seconda sessione ha avuto ad oggetto le tecniche di contrasto al fenomeno dei crimini economici nell'era della digitalizzazione mentre nell'ultima sessione è stato affrontato il problema dell'uso dell'intelligenza artificiale nella procedura penale.

Il corso si è svolto interamente in lingua inglese con la traduzione contestuale in turco, arabo e francese.

I sottoscritti sono stati entrambi apprezzati *speakers* in lingua inglese sulle tematiche del rapporto tra intelligenza artificiale e criminalità (Lettieri) e su quella dell'esperienza italiana nell'acquisizione ed utilizzazione della prova digitale (Baldi).

L'incontro è stato in ogni caso molto proficuo per la maturazione di una serie di contatti, in particolare con Argentina, Austria, Belgio, Marocco, Svizzera e Turchia, sicuramente preziosi per lo sviluppo dell'attività internazionale dell'Ufficio.

Nell'occasione, gli scriventi, previa organizzazione di un bilaterale a margine del *meeting* principale, hanno incontrato il Segretario Generale dello IAP, Han Moraal, il quale, nell'illustrare le condizioni per l'ingresso dell'Italia nell'Associazione Internazionale dei

Pubblici ministeri, già esplicitate in una precedente corrispondenza intrattenuta col nostro Ufficio e da lui citata nel corso dell'incontro, ha espresso l'auspicio che tale adesione avvenga entro il prossimo *meeting* annuale che si terrà a Londra da 24 al 27 settembre 2023. Il predetto ha specificato che l'adesione prevedrebbe condizioni economiche - comunque da sottoporre all'assemblea dei membri per l'approvazione - a suo giudizio molto favorevoli (nella stessa entità applicata all'Ungheria), segnatamente: un importo annuale di Euro 2000 per il primo anno, di Euro 4000 per il secondo, di Euro 6000 per il terzo, di Euro 8000 per il quarto, mentre dal quinto anno in poi il costo si cristallizzerebbe in Euro 10.000 annui. Al riguardo si suggerisce un'interlocuzione con il Capo del Dipartimento degli Affari Giustizia, dott. Birritteri.

Si resta a disposizione per ulteriori chiarimenti.

Si allega la locandina dell'incontro.

Roma, 8 maggio 2023

Dr. Nicola Lettieri



Dr. Fulvio Baldi



The use of A.I. as a tool for committing crimes.
The use of A.I. for fighting crime and obtaining evidence.

by Nicola Lettieri

Deputy Attorney General at the Italian Court of Cassation
Istanbul May 2023

I. Advancements in artificial intelligence have reached such a terrifying new level that they allow criminals to replicate a voice with an audio sample of just a few sentences. Cheap A.I. tools can translate an audio file into a replica of a voice, thus allowing a swindler to make it “say” and “talk” whatever he wants. In other words, A.I. can transform a short vocal sample into a synthetically generated voice through a text-to-speech tool.

By using A.I., criminals manage to persuade people, especially elderly people that their loved ones are in distress. A criminal who pretends to be a friend of his grandson may call an old man and let him listen to a perfect replica of his grandson’s voice. The voice says (that) he is in jail, with no wallet or mobile and needs cash for bail. At that point, the old man is available to do whatever he can to help: he goes to his bank, withdraws the daily maximum amount, and hand it over to the swindler. Just a short time after that, he realizes he was duped. This kind of fraud is very popular not only in Italy: for instance, it is the second most popular crime in the Unites States of America, with over 36,000 reports of people being swindled by those pretending to be friends and family members.

Many victims are vulnerable subjects; therefore, they are reluctant to report. When they do so, the police and courts are ill-equipped to tackle this phenomenon, even because most victims have few leads to identify the perpetrator and it is difficult for the police to trace calls and funds from scammers operating across the world. This kind of swindlers could use a phone based anywhere in the world, making it hard to even identify which country has jurisdiction over a particular case. It can also happen that the swindler’s call comes from a family member’s number, just because the number has been spoofed.

II. The above example concerns lower level criminals and massive crimes, but A.I. could also be used for other unlawful and more sophisticated purposes, such as:

a) the *deep fake* technique, that is to replicate voices of politicians saying things they never did for the intended purpose to destabilize a country or a political party or to rig an election or to delegitimize a political opponent; the same can happen with A.I. applied to fake videos or photos;

b) in the event of wiretapping, the purpose is to replicate voices of some people in order to turn responsibility for crimes under investigation away from themselves and make

others responsible for their criminal conducts (let us think of some captured chatter indicating drug-trafficking);

c) in the context of economic crimes, notably stock-market manipulation, we can have:

i) Dissemination of false news through social media that are capable of influencing the volatility of securities, social bots (that is a software that simulates to be human users and communicates autonomously on the social media) can be used for the *pump and dump*. This is a particular type of fraud which consists in artificially increasing the price of a security with a basically stable price, by making false, misleading or exaggerated statements, with the aim of selling securities purchased cheaply at a higher price;

ii) *Spoofing*, when an investor places a large buy order, only to cancel it and place a sell order. The buy order drives the price of the security up, while the sell order takes advantage of the higher price. The algorithm¹ will cancel such buy order before it is fulfilled and, meanwhile, enter a sell order at prices that by now must have been affected by demand-side pressure, thereby profiting at the expense of other investors².

III. The previously mentioned cases are just some examples of possible harmful use of A.I.

As for the challenges to counter these dangerous unlawful phenomena, we can summarize the following issues:

1. Jurisdiction problems related to the transnational nature of the phenomenon. Virtual space or cyberspace cannot be assimilated to any of the realities we have known up to now. This dimension looks like those of “Universal Jurisdiction”, theorized in the Humanitarian Law, or the “High Seas”, where two principles of international law are established. “Freedom of High Seas”, i.e. high seas in time of peace, which are open to all nations and may not be subjected to national sovereignty, and “Flag State principle”, according to which a ship on the high seas is exclusively subject to the jurisdiction of its flag State. By analogy, each State has the right of use and economic exploitation of the cyberspace, with the only limit of respecting the equal right of any other State. This amounts to saying that courts can exercise national jurisdiction on cybercrimes using criteria other than territoriality.

¹ More advanced algorithms can use conditionals to divert the code execution through various routes (referred to as automated decision-making) and deduce valid inferences (referred to as automated reasoning), achieving automation eventually.

² With the aim to avoid any possible sort of manipulation of the market, see Regulation (EU) No 596/2014 of the European Parliament, and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC.

2. Anyway, the establishment of its own jurisdiction is in principle quite different from actually exercising jurisdiction. If someone asserts to have jurisdiction in this domain, without the judicial cooperation of other countries, it is a mere exercise in style. Indeed, investigation can lead to people operating under the territorial jurisdiction of another State, or in any case to such sovereign subjects and, moreover, speed in obtaining evidence of this kind of illegal conduct is essential in investigating cybercrimes. In this event, if evidence points to people living in other countries, where networks, servers and clouds are based, you obviously need judicial and efficient cooperation.

3. Then, considering that criminals and algorithms can be virtually placed in countries where the phenomenon is not criminalised or in countries which have no interest in fighting cybercrimes producing harmful events occurred abroad, the harmonization of the legislations at a supranational level is crucial, in order to gather evidence and information through judicial cooperation tools. Recent European Parliament's resolutions³ urge the establishment of a common European legal framework for the use of A.I. with harmonized definitions and common ethical principles. They should point out that A.I. must be subject to some meaningful human control, so that a human being has the means to correct, halt or disable it at all times, in the event of unforeseen behaviour, accidental intervention, cyber-attacks or interference by third parties with AI-based technology or in any case third parties acquire this technology.

4. This attention to the human control is justified by the following principle: if AI-enabled systems must allow humans to be in charge and exert meaningful control, they assume full responsibility over the systems, and they can be accountable for all their uses. However, you must take into account that one facet of human intelligence is the ability to learn from experience. Machine learning is an application of A.I. that mimics this ability and enables machines and their software to learn from experience (for instance, self-driving cars or a system that can learn the practice of financial spoofing, i.e. it can place orders). This can happen through the cloud computing system, which

³ Resolutions of the European Parliament on this matter.

a) 2015/2103 (INL) of 16 February 2017 on civil matters concerning A.I.; b) 2020/2012 (INL) of 20 October 2020 on the framework of ethical aspects of artificial intelligence, robotics and related technologies;

c) (2020/2014(INL) of 20 October 2020 on civil liability regime for artificial intelligence;

d) 2020/2015(INI) Report on intellectual property rights for the development of artificial intelligence technologies;

e) 2020/2013(INI) of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and state authority, outside the scope of criminal justice;

f) 2020/2016(INI) of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters.

See also The Charter of Fundamental Rights in the context of Artificial Intelligence and Digital Change, by the Council of the European Union, Presidency conclusions, 11481/20, of 21 October 2020.

enables to access applications and data remotely. By means of cloud computing technologies, if an AI-enabled system exchanges information with other systems, it can exponentially increase its own learning. Some implementations of machine learning use data and neural networks in a way that mimics the working of a biological brain. Then, it is clear that the behaviour of such AI-enabled systems is not entirely predetermined, and therefore foreseeable. As a result, it could be problematic to identify a human to blame for a crime occurred because of such a conduct.

5. Some legal scholars urge the introduction of new types of crime or aggravating circumstances. By Law No. 48 of 18 March 2008, the Italian Legislator ratified the so-called Budapest Convention⁴, and introduced new cyber-crimes in the national legislation. This seems not to be enough. Indeed, especially with respect to economic crimes, some think that A.I. companies should be held liable if their products are vectors for crimes. This happens because trading is frequently done in high volumes and at high speeds by several employees of companies, using complex computer systems. If such a conduct occurs on behalf of the company, it should be fair the attribution of the liability for market manipulation to the company, by applying the rules relating to the agency contract.

IV. Anyway, not only criminal reality, but also public safety and criminal justice can benefit from A.I.

Let us think of the possibility of using artificial intelligence in investigative work, where self-learning algorithms use data sets to understand how to identify people based on their images (there is a dedicated software called S.A.R.I.). A.I. algorithms are improving detection, recognition and identification, by working even on images with poor resolution and low ambient light levels, where the image quality makes facial matching difficult.

A.I. is also quickly becoming an important technology in fraud detection: Internet companies like PayPal stay ahead of fraud attempts by using volumes of data to

⁴ The Budapest Convention is a treaty of the Council of Europe (23/11/2001) open for signature by member States and non-member States, which have participated in the drafting, and for accession by other non-member States. It is more than a legal document, rather a framework that permits hundreds of practitioners coming from the Parties to share experiences and create relationships that facilitate cooperation in specific cases, including in emergencies, beyond the specific provisions foreseen in this Convention.

Since the powers of law enforcement are limited by territorial boundaries, the Second Additional Protocol to the Convention responds to this challenge. It provides tools for enhanced co-operation, and disclosure of electronic evidence - such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations - that are subject to a system of human rights and rule of law, including data protection safeguards.

continuously train their fraud detection algorithms to predict and recognize anomalous patterns and to learn to recognize new patterns.

Another important aspect of AI is the ability to predict behaviour. Scholars are developing algorithms that provide continuous monitoring to assess activity and predict emergent suspicious criminal behaviour across a network of cameras. This work also concentrates on using clothing, skeletal structure, movement, and direction prediction to identify and reacquire people of interest across multiple cameras and images.

A.I. is also capable of analysing large volumes of criminal justice-related records to predict potential criminal recidivism.

V. In conclusion, it is the eternal struggle between the sword and the shield: the more criminals progress in exploiting A.I. for illicit purposes, the more A.I. is evolving to be a permanent part of our criminal justice ecosystem, providing investigative assistance, and allowing criminal justice professionals to better maintain public safety.

Istanbul 2-5 May 2023. Speech of Mr. Fulvio Baldi, Deputy Prosecutor General at the Supreme Court of Cassation, Italy.

“Gathering and use of digital evidence in criminal procedure in the context of effective investigation; illegality problem in digital evidence” – the Italian experience

§ 1 - As it is well known, digital evidence represents a very important sub-category within the category “scientific evidence”, defined as it is by two features:

Digital trails are fragile, as they can be easily modified, damaged and destroyed. The fragility of digital trails is innate and inevitable. It does not depend on possible intentional manipulations or eventual accidental behaviors of the persons dealing with them. The casual loss of data is so frequent that it turns into a problem; hence, we need to find adequate solutions.

To this end, the Italian Law No. 48 of 18 March 2008 ratified and put into force the Convention on Cybercrime of the Council of Europe, signed in Budapest on 23 November 2001.

§ 2 – In the matter of search and **acquisition of evidence**, regulatory provisions on inspections, searches and seizures conducted by the public prosecutor or - as a matter of urgency- by the (judicial) police were modified to make specific adjustments to IT realities.

When judicial authorities conduct inspections, or searches of IT or electronic systems, they must adopt “technicalities tending to ensure the preservation of original data and prevent their alteration”. According to the said rules, it is mandatory to adopt procedures ensuring the integrity of digital data, following Judicial Authorities’ interventions, thus protecting the right to defense.

The acquisition of computer data is provided for “by the means of a copy... on an adequate support, with a procedure ensuring that obtained data have to be consistent with original data, and they cannot be modified”. Indeed, technically, the term copy is not reassuring at all. A copy allows you to duplicate data or their contents

from a support (i.e. any mass memory, such as a hard disk or a pen drive) to another support. However, it does not guarantee, for example, the same data location on the support (the so-called forensic copy).

In the matter of search for evidence, police officers can proceed to search IT systems, even if they are protected by security measures, in case of flagrante delicto, or when an order for preventive custody in prison or an execution order has being enforced.

The Legislator also ruled on the subject of seizure of correspondence. It established that Judicial Authorities are responsible for seizing letters, parcels, packages, valuables, telegrams and other kinds of correspondence at the postal, telegraphic, telematics or telecommunication service providers, even if they are sent via e-mail.

It was underlined how the rule under consideration raises an interpretation issue of no less importance; can e-mails or SMS/MMS messages be seized? The literal interpretation of the new Article 254 of the Code of Criminal procedure would actually seem to allow such an interpretation. In Italy, it is known by now that SMS/MMS are seized and used.

A new Article, i.e. Article 254 *bis* of the Code of criminal procedure, was also introduced. This Article establishes that Judicial Authorities may obtain data through copies, when they conduct seizures of the data owned by digital, telematics or telecommunication service providers, including traffic and location data, for purposes of regular provision of services. Service providers are responsible for the preservation of original data. One problem is that the procedure is optional and not mandatory.

§ 3 - With reference to **the possibility of using them**, the Italian Supreme Court of Cassation held that a copy taken from a digital document has the same probative value as the datum originally acquired, unless some manipulation is deduced and proved (Cassation, No. 12975 of 6 February 2020). As it was stated, video-recordings of security systems represent digitally obtained and saved documents. This allows you to make identical reproductions in an indefinite number of specimens to be used as full proof, unless some manipulation has been deduced and proved. In fact, the transfer to

file or the extraction of images does not alter in itself the data stored on the server. Therefore, the copies thus obtained have the same probative value as the data originally acquired (Cassation, No. 15838 of 20 December 2018).

According to the Italian Supreme Court, the extraction of data stored in an IT device, such as a mobile phone, does not represent a technical assessment that cannot be repeated. In fact, the 2008 Law, ratifying the Budapest Convention, only introduced an obligation to adopt suitable collection methods, ensuring the consistency of digital data with original data. Therefore, neither the failure in obtaining these data, nor the lack of communication with the parties thereto result into not using the probative results thus obtained, without prejudice to the need for assessing, in practice, the existence of any alteration of the original data and the correspondence of extracted data to them (Cassation, No. 38909 of 10 June 2021).

In the matter of probative seizure, the Supreme Court of Cassation has ruled that the seizure of an entire personal computer shall be considered lawful and not against the principles of proportionality, suitability and gradualness, rather than the extraction of individual data. This happens when the seizure is justified by technical problems in extracting, with targeted reproduction, data from the memory (Cassation, No. 38456 of 17 May 2019).

For the Supreme Court of Cassation, e-mails that are not sent by the user, but saved in the file "drafts" of one's account, or an appropriate virtual space (such as Dropbox or Google Drive) represent digital documents that can be seized (Cassation, No. 40903 of 28 June 2016).

With respect to precautionary seizure, the Supreme Court has also held that Judicial Authorities can order a precautionary seizure of an entire website or an individual web page, as appropriate. Thus, they can impose on the internet service provider, also as a matter of urgency, to take an electronic resource down or prevent users from accessing it. In fact, the equivalence of computer data to things, in a legal sense, helps prevent the availability of the information on the Net, as well as the prolongation of the harmful consequences of a crime (Joined Chambers of the Supreme Court, Judgment No. 31022 of 29 January 2015).

The Supreme Court of Cassation has established that the usage, for precautionary purposes, of chats on the "Sky Ecc" and "Encrochat" systems is legitimate. The chats were obtained, via investigation order, from a foreign authority who deciphered them, considering that it distinguished between the concept of conversation decryption and the concept of conversation reception. It has stated that you can acquire a plain digital datum, obtained by the transfer of the "strings" into easy-to-read contents, by the means of the relevant algorithm provided for by the company who owns the operating system (Cassation, I Chamber, No. 6363 of 2023).

§ 4 - The rules in question date back to 15 years. They were enacted without any special reference to technicalities for the collection and preservation of digital evidence. On one hand, the legislation can remain valid, despite the ongoing development of IT technologies, and there is no need for the legislator to make continuous "run-up" interventions. However, on the other hand, all this leads to huge interpretation gaps that you can easily imagine, when you think of the digital supports for investigation: computers, laptops, and not particularly developed mobile phones. Above all, most data were saved in the physical memory of the device under examination. Today, instead, we deal with tablets, Clouds, and smartphones working like real computers of good quality.

§ 5 However, as a result of the Legislative Decree No. 216 of 29 December 2017, another means for the search of evidence, i.e. the Trojan horse, supplemented these rules. Conversations among those present can always be tapped, by inserting a Trojan horse in an electronic portable device, in the case of proceedings for crimes against organized crime and the civil service, when the public Prosecutor must request the authorization for inserting a Trojan horse to the Judge for the preliminary investigation. With a reasoned decree, the public Prosecutor may order to tap those present, by inserting a Trojan horse in a portable electronic device, as a matter of urgency. However, he must forward this order to the Judge who decides on its validation. With respect to the possibility of using and validating the results thus acquired, it is expressly stated that the results of the present persons' tapping through a Trojan horse, fixed on a portable electronic device, cannot be used to prove crimes rather than the crimes for which the authorization decree was issued. That is, unless they are indispensable for the investigation of crimes

for which the arrest in flagrante delicto is mandatory. Instead, in no case, you can use the data obtained in the course of the operations, before inserting the Trojan horse in the portable electronic device, and the data obtained outside the time and space limits mentioned in the authorization decree.

The Supreme Court of Cassation has established that recording activities, i.e. the entry of captured data in a centralized digital memory- according to currently used technologies- must take place in the Prosecution Office's premises, as a pre-requisite for the possibility of using wire-tapping. Devices already existing therein should be used. It does not matter if digital devices used for capturing communications among those present do not automatically transmit audio-recorded files, but the files shall be periodically collected by the (judicial) police in charge of the operations, and hand-poured into the server of the Prosecution Office (Cassation, No. 34671 of 26 October 2020). Likewise, it does not matter if further listening activities, the taking of minutes and any reproduction of data thus recorded are also carried out later on in the same premises, as they can be accomplished "remotely" within the premises of the (judicial) police (United Chambers, Judgment No. 36359 of 26 June 2008). The Judge in chambers can listen to any recordings in the analogic or digital devices, which are duly acquired, and written down in transcripts, and he can use them to take a decision based on the results of his listening (No.22062 of 24 April 2013). The lack of the full name of the officer, installing the "spyware" (*captatore informatico*) through a Trojan horse in the transcript concerning the execution of the tapping operations, does not mean that the results of the tapping operations cannot be used (Cassation, No. 32426 of 24 September 2020).

The Supreme Court of Cassation has also stated that the non-release of the copy of the tapping's audio files, required to spot manipulations or interventions on the texts with alterations of the original trails, does not imply that the results of the tapping cannot be used, since there is no specific law provision sanctioning it accordingly. These (Cassation, No. 50021 of 12 December 2017).

At the same time, the Court has stated that the transcript of the finished operations still in digital format, without the subsequent printing or transposition on paper, hence without the signature of the

public official who drafted it, does not entail its invalidity or non-existence (Cassation., No. 27112 of 07 July 2020).

According to the Supreme Court of Cassation, the tapping of computer or telematics communications, carried out by installing a spyware (the so-called "Trojan horse") inside a computer located in a private abode (Cassation, No. 48370 of 30 May 2017) or in a public office is legitimate (Court of Cassation, No. 16556 of 14 October 2009). It is also legitimate to acquire a file, whose editing is ongoing on a personal computer, by using a screenshot taken by a Trojan horse (Cassation, No 3591 of 07 October 2021).

Environmental tapping through a "Trojan horse", installed in Italy on a telephone connected to a national company, does not require the sending of an international letter of request, for the only reason that the conversations are partly carried out abroad, and temporarily recorded via Wi-Fi locally, because of the transfer of the device onto the malware is inserted. In fact, the reception originated, and in any case took place in Italy, through the reception stations at the Public Prosecution Office (Cassation, No. 29362 of 22 July 2020).

Istanbul, 3/5/2023

A handwritten signature in black ink, appearing to be 'Fulh RL', written in a cursive style.