Chambers

GLOBAL PRACTICE GUIDE

Definitive global law guides offering comparative analysis from top ranked lawyers

eDiscovery & Disclosure

Italy
Paul Hastings (Europe) LLP

chambers.com

2019

Law and Practice

Contributed by Paul Hastings (Europe) LLP

Contents

Paul Hastings (Europe) LLP has an eDiscovery team in Milan, consisting of two partners, four associates and two trainee associates, with other key office locations in Los Angeles and New York as part of a wider network. The primary practice areas related to the eDiscovery sector are white-collar and internal investigations, compliance (anti-bribery and Law 231, anti-money laundering and market abuse) and data protection law. The compliance and investigations practice encompasses all aspects of compliance and assists a wide range of clients, such as leaders in the industrial and financial services sectors. It has advised the US group world leader as well as other multinational groups in the treatment of rare diseases in its compliance and anti-corruption assessment aimed to ensure compliance with local and international anti-corruption laws. The firm is advising one of the world's leading multinational oil and gas companies on market abuse regulation-related compliance. It often provides training in compliance matters, as well as data protection, for members of boards of directors and key management from corporations.

Authors

Bruno Cova, a partner, is the head of corporate in the Milan office and chair of the Milan office. He focuses his practice on M&A, securities law, corporate governance and compliance, energy matters, restructurings and complex cross-border litigation. Mr Cova has international experience of leading the legal functions of major global companies and advising top executives on global expansion as well as corporate crises. He is a member of the troika of experts advising the Corporate Governance Committee of the Italian stock exchange on corporate governance reforms, a member of the High Yield Insolvency Committee within the Association of Financial Markets in Europe, co-chair of the Anti-Corruption Committee of the International Bar Association and a member of the editorial board of Global Investigations Review, a leading economic and law publication focusing on the law and practice of international investigations.

Francesca Petronio is a partner and the head of litigation in the Milan office, with extensive experience in cross-border disputes and litigation, domestic and international arbitration, bankruptcy and corporate litigation matters. She specialises in white-collar crime, administrative and criminal liability, and compliance matters under Legislative Decree 231/2001, assisting domestic and international clients in internal investigations and defending them before regulatory authorities or in the context of criminal investigations. She has been a member of the Milan Bar Association since 1997, is an officer of the International Bar Association and quality officer of its Anti-Corruption Committee, and is admitted to practice before Italy's Supreme Court of Cassation. A lecturer at the National School for In-house Counsels of AIGI since 2011, she was a co-founder of the Arbitrando association.

Marilena Hyeraci is a senior associate with extensive experience in litigation, civil and commercial matters, criminal corporate law and data protection, having advised clients on pre-litigation issues and the assessment of legal risk, as well as the development of compliance models and anti-corruption systems. Leading Italian and multinational companies have been guided on matters concerning white-collar crimes, corporate liability, internal investigations and liability proceedings against corporate directors. She has advised clients on establishing privacy compliance programmes, pursuant to the General Data Protection Regulation, and provides counsel on responding to suspected security breaches and personal data disclosures to the authorities. She is a member of the International Association of Privacy Professionals (USA), the Federprivacy/Privacy Officer Association (Italy) and the Milan Bar Association, and a lecturer at the National School for In-house Counsels of AIGI since 2013.

Giulia Fiorelli is an associate in the corporate department of the Milan office who focuses her practice on M&A, restructuring transactions, private equity and general corporate matters, advising Italian and international clients on domestic and cross-border transactions as well as internal investigations.

1. Litigation System

The Italian litigation system is a civil law system. The main rules governing commercial relationships are embodied in the Italian Civil Code, which was enacted in 1942, and in other special laws. It is worth clarifying that the Italian legal framework provides for specific rules for administrative and criminal proceedings.

Specifically, the Italian civil litigation system is a multi-tiered judicial system, which provides for an appellate system, whereby a decision of the Court of First Instance, the court that considered the case on its merits for the first time, can be appealed to the Court of Appeal and, ultimately, to the Italian Supreme Court.

The litigation process is governed by the Italian Civil Procedure Code. To summarise, the main courts in civil matters are as follows.

- The Justice of the Peace (*Giudice di Pace*) – this has jurisdiction, as Court of First Instance, over minor civil matters (and minor criminal offences) in a specific area.
- The Ordinary Court (*Tribunale*) – this is the Ordinary Court of First Instance with jurisdiction in a specific geographic area (except for the Justice of the Peace with reference to minor proceedings). As a consequence, the Ordinary Court is also the first level of appeal against the decisions of the Justice of the Peace. Such courts may be composed of three judges or a single judge.
- The Court of Appeal (*Corte di Appello*) – the decisions issued by the Courts of First Instance can usually be appealed before the Court of Appeal. The procedure permits a new examination of the points of the dispute that have been challenged and, thus, may lead to a complete re-examination of the case. In addition, the appeal of the first instance decision prevents that decision from becoming res judicata and under certain circumstances, the new decision on appeal 'substitutes' the first instance decision.
- The Supreme Court (*Corte di Cassazione*) – the decisions issued by the Court of Appeal can generally be challenged before the Italian Supreme Court, which mainly verifies the proper application and interpretation of law by the Court of Appeal in reaching its decision (assessment of legitimacy). Such court cannot overrule the Court of Appeal's interpretation of facts and evidence collected. Its offices are in Rome and it has jurisdiction over the whole territory of the Italian Republic.

2. Electronically Stored Information (ESI)

As a consequence of the advent of electronic media platforms and the development of a globalised marketplace, the majority of documentary evidence relevant to civil litigation, investigations and arbitration is now in electronic form, commonly referred to as electronically stored information (ESI).

Specifically, ESI can be defined as any information that is created or stored electronically (eg, writings, drawings, graphs, charts, photographs, sound recordings, images and other data). ESI can be found on laptops, smartphones, tablets, corporate shared devices, internal servers and platforms, voicemail systems and, more generally, anywhere electronic data can be accessed, saved or downloaded. The possible types of ESI grow daily, as new technologies are implemented and new types of data are produced.

In this context, however, only the USA and a few other countries have adapted their legal systems to address the discovery or disclosure of ESI by introducing specific rules and procedures for its production as well as protection of relevant privileged information.

The Italian legal framework does not provide for specific rules or procedures relating to the discovery and disclosure of ESI, and most of the new technological tools are little known in Italy. Indeed, several technological tools for the collection of electronic documents and data have been developed (eg, data integration platform, virtual data room, tools to preserve documents in real time, tools to recover entire mailboxes including deleted data), with several advantages in terms of time and cost savings, when a large amount of documents must be managed and several countries are involved in the procedure.

3. Case Law or Rules Relating to ESI

The Italian legal system is still rather unfamiliar with ESI. In this field, there is neither national regulation nor standards of practice. To date, no cases involving ESI have been made available by public sources and legal scholars have not properly addressed this topic.

Against this background, the Italian litigation system has recently experienced a radical change: several initiatives have been implemented to increase the efficiency of the Italian legal system and speed up the proceedings, in particular, by means of a 'digitalisation' of them (eg, Decree of the President of the Republic No 123/2001, Decree No 44/2011, Law No 228/2012 and Decree No 90/2014).

4. Discovery/Disclosure of ESI

As already mentioned, the Italian legal system does not provide specific rules relating to the discovery and disclosure of ESI as, for instance, the USA does. However, the use of certain technological tools to manage judicial proceedings has been introduced with the implementation of the Civil Telematic Process.

The Civil Telematic Process has been implemented with the aim of improving the quality of services in civil proceedings. In particular, the excessive length of trials was determined to be the primary reason behind its implementation. By means of this new technological architecture, activities that previously required physically going to the court – including document filings, notifications, communications and consultations regarding proceedings status – can now be handled online, with significant savings of time and costs. In addition, judges benefit from this new process as well: court decisions are now written directly using the telematic panel and are issued digitally.

One of the first steps leading to this digital transformation was implemented in 1997 when the fundamental instruments involved in telematic proceedings were identified and the criteria and means for the processing, storing and transmission of documents through electronic devices were established (Presidential Decree No 513 of 10 November 1997 implementing Law No 59 of 15 March 1997 "concerning the creation, storage and transmission of documents by means of computer based or telematic systems," or the 'Decree').

The Decree provides for a mechanism of 'validation' of documents by means of a digital signature, defined as a computer-based cryptographic system capable of creating and affixing digital signatures or of verifying the validity of digital signatures, which allows the signer and the recipient respectively to prove and verify the document's source or integrity. In addition, it regulates a set of hardware and software, by which the judicial administration manages, among other things, all data, services, communications and procedures.

Afterwards, the electronic document will be properly defined as any representation of act, fact or data in a legally relevant digital format. The judge is always free to evaluate an electronic document's validity by considering its integrity, quality and authenticity (Decree No 82 of 3 July 2005).

In 2009 the regulation of telematic proceedings was extended to criminal trials and, beginning in 2009, all digital communications and notifications require 'certified email'. Specifically, certified emails (PEC) provide to the sender a receipt attesting to the delivery, certifying date and time of the dispatch. As provided by the law, the adoption of certified email is compulsory for lawyers, public entities and companies (Decree No 193/2009).

Since then, the regulation of the telematic process in civil and criminal proceedings has been aligned. Additionally, Italian bankruptcy law has been modified to permit the use of certified email in insolvency proceedings. From 30 June 2014, the electronic filing of all the civil proceedings documents became compulsory, providing that in case of any malfunction or breakdown of the system, the judge can permit the filing of paper versions (Decree No 179/2012 and Law No 228/2012)

Electronic documents can be signed in different ways. According to the specific tools used, the documents signed can be considered (i) a mechanical reproduction pursuant to Article 2712 of the Italian Civil Code or (ii) a private writing with the effectiveness provided by Article 2702 of the Civil Code, according to which the private writing is considered authentic, unless a false complaint is filed.

It is worth mentioning that in this context several 'technical' formalities shall be followed to be in compliance with the regulations relating to the signing, transmitting and receipt of electronic documents, and effectively to manage the access to digital data and their filing (among others, as provided by the Decree of 17 July 2008 and after Decree No 44 of 21 February 2011 – "Regulation relating to technical rules for the adoption of digital information in civil and criminal proceedings").

Going forward, all trials shall be handled entirely electronically, from the filing of pleadings to the notification by the courts of hearings and decisions. Such digitalisation has realised a decrease in the length of proceedings and a benefit for the professionals and parties involved in the proceedings, with a simplification of the judicial procedures.

5. Obligations to Preserve ESI

Italian law does not provide for a duty of disclosure and discovery of ESI, nor does it provide a duty to preserve it. In the absence of a specific regulation concerning ESI, the provisions relating to the duty to preserve legal documents, whether in digital form or not, shall apply.

Specifically, courts shall preserve the legal documents until the end of the judgment or until the claim is declared inadmissible. After the conclusion of the proceedings, the Italian Civil Code provides that courts, lawyers and arbitrators must preserve all legal documents for three years after the decision or the termination of the lawsuit (Article 2961 of the Italian Civil Code).

In fact, despite the foregoing, lawyers are required to preserve client documents for ten years, as provided under Article 2946 of the Italian Civil Code. It must be noted that lawyers may keep a copy of any documentation provided by the assisted party. However, upon request of the client, lawyers shall return without delay any documentation received from the client or the assisted party in connection with his or her representation. Additionally, the attorney shall not withhold the return of any or all requested documents to the client, even if said attorney has not yet received full compensation (Article 33 of the Code of Conduct for Italian Lawyers – *Codice Deontologico Forense*).

The modalities for the storage and conservation of digital and electronic documents are not without challenges. Since the storage of electronic documents is more complex than of paper documents, lawyers often outsource the management of electronically stored documents (which, in turn, may be dangerous for the clients' privacy) to a 'specialised entity' that is capable of handling huge amounts of sensitive information. In such cases, the balance between the need to preserve digital documents with the protection of clients' privacy represents a critical and delicate issue.

In several cases, specific discipline regarding specific duties in relation to the preservation of legal documents according to the particular sector/industry of interest should apply. Such rules often only provide for the preservation's modality, without any reference to the duration of the obligation.

6. Sanctions and Penalties

Since the Italian legal framework does not specifically recognise ESI as a unique procedure for the maintenance of electronically stored information, or provide specific regulations, there are no provisions relating to the preservation of ESI and the imposition of sanctions or penalties for failure to preserve them.

Nevertheless, the Code of Conduct for Italian Lawyers (*Codice Deontologico Forense, or* the 'Code') does provide some guidance. Although the Code does not provide for any specific rule on the obligation to preserve legal documents, it establishes specific disciplinary sanctions against any lawyer who fails to return documents when requested by the client or who deliberately withholds the return of any and all requested documents to the client, because said attorney has not yet received full compensation.

Specifically, the breach of the duty provided under Article 33 of the Code entails the enforcement of the following disciplinary sanctions. First, a warning (*avvertimento*), which shall apply if the lawyer fails to return the documents upon the client's request. It consists of informing the accused that his or her conduct has not complied with the rules of ethics/law, cautioning him or her to refrain from carrying out other infractions. Usually such a disciplinary sanction applies to non-serious violations, if there are reasons to believe that the accused will not commit other infractions. Second, censure (*censura*), which shall apply if the lawyer deliberately withholds the return of any or all requested documents to the client, because said attorney has not yet received full compensation. It consists of a formal reprimand and applies when (i) the gravity of the infraction, (ii) the level of responsibility, (iii) the previous behaviour of the accused lawyer and (iv) his or her behaviour following the infraction lead to the belief that he or she will not commit another violation.

Notwithstanding the foregoing, in several cases, other additional rules (to be determined on the basis of the sector of interest) providing for specific sanctions or penalties shall apply (eg, the privacy regulation).

7. Timing and Extent of Sanctions

The Italian legal framework does not provide specific regulations for the preservation of ESI, nor for the imposition of sanctions or penalties for failure to preserve them. Nevertheless, the Code of Conduct for Italian Lawyers (*Codice Deontologico Forense*) does provide guidance (see **6 Sanctions and Penalties**).

In addition, other specific rules according to the sector of interest may apply (eg, the sanctions set forth by the privacy regulation).

8. Costs of Discovery/Disclosure of ESI

Although the Italian legal system does not provide any specific rules relating to the discovery and disclosure of ESI, it is worth noting that the Italian civil litigation system is based on the 'loser pays' principle, according to which, the judge orders the losing party of the proceedings to pay the legal fees and expenses of the winning party (Article 91 of the Italian Code Civil Procedure).

Specifically, these costs, which include court administrative expenses and lawyers' fees, are calculated on the basis of the amount of the dispute itself.

The lawyers' fees are calculated as provided by Ministerial Decree No 55/2014, which sets out the parameters and criteria for the calculation of fees on the basis of, among other factors, the complexity of the proceedings, their value and the number of parties involved. To the lawyers' fee should be added the court administrative costs and legal charges (value added tax, usually 22%) and a mandatory contribution to the lawyers' pension fund (CPA, 4%).

In the event that both parties partially lose, the judge can offset or balance, totally or partially, the litigation costs between the parties.

9. Obligations of Parties to Meet and Confer

As mentioned, there are neither national regulations nor standards of practice in relation to ESI. It goes without saying that there are no mandatory requirements relating to the communications between the parties in relation to ESI and the disclosure of e-documents similar to the requirements of US Federal Rule of Civil Procedure 26(f).

In this context, according to the Italian legal system, the parties do not exchange written evidence from witnesses or experts before trial. Specifically, prior to trial, the parties do not exchange any documents. In cases of urgency (eg, if there is a well-founded risk that a witness may die) the parties may demand that evidence be taken before the beginning of the trial or request verification of the status of certain sites or the condition of specific items and may also require a technical assessment or judicial inspection prior to trial.

Therefore, the court cannot impose any orders on the parties in relation to any 'pre-action' activities, except if the assisted negotiation and the mediation procedures are mandatory before the commencement of the proceedings. In particular, to reduce the number of Italian proceedings, Legislative Decree 28/2010 provides that, under certain circumstances, the parties, before commencing any judicial proceedings, shall first attempt to settle the dispute by means of a mediation procedure (mandatory mediation).

The assisted negotiation procedure, introduced in 2014, is another mandatory out-of-court procedure for the settlement of the dispute that shall be implemented by the parties in certain circumstances before commencing the proceedings before the court.

10. Scope of Party's Obligation Regarding Electronic Documents

As mentioned, the Italian legal framework does not provide any specific obligation of the parties to search for, disclose and produce electronic documents (ESI).

However, in the context of criminal investigations – in particular, involving Italian companies belonging to a US group – identifying the scope of the investigation is probably the key part of the process, even in the absence of any specific obligations on the parties.

Although it is difficult to predict accurately all the phases of the investigation process, which are usually defined as the investigation progresses, it is advisable to limit the scope of an investigation to the allegations and to avoid investigation activities 'out of scope' without a specific need. In addition, the scope of an investigation can always be extended at a later stage if needed.

11. Requirement to Certify that Search Carried Out

The parties are free to disclose evidence. The parties can request the judge to order the production of documents to specific third parties in order to gather specific evidence and the court can order the disclosure to any party involved in the proceedings or to a third party, if deemed appropriate.

At the same time, the parties may challenge the order to disclose certain documents for specific reasons, such as medical or bank privacy, or legal privilege.

There are several restrictions on the disclosure of confidential documents covered by legal privilege and of documents with sensitive and personal data. As mentioned, an electronic document, signed with a digital signature in the proper manner, satisfies the legal requirement of written form.

The parties shall not file any confidential correspondence with their counsel regarding a possible settlement of the dispute, with the exception of the correspondence regarding the fulfilment of the obligation(s) in favour of the counterparty.

12. Form of Production of ESI

There are several principles that should be borne in mind by the parties and their legal representatives as well by the 'processing party' in relation to the production of electronic documents, given that the Italian legal framework does not provide any specific rules relating to the production of ESI as in other jurisdictions.

As previously mentioned, the process for the validation of electronic documents is crucial to their production in civil proceedings. The digital signature may be affixed or associated by means of a separate document to electronic documents. Affixing a digital signature to an electronic document or associating one with it shall have the same effect as putting the required signature to written acts, documents or paper. A digital signature identifies the signatory, the authority that carried out the certification and the repository where it is accessible for consultation. A private key shall be used to generate a digital signature. Using a digital signature by means of a revoked, suspended or expired key shall have the same effects as failure to sign.

A digital signature can be authenticated by a notary public or another authorised public official and in such case shall be deemed to be an authenticated signature as provided by Article 2703 of the Civil Code. In order to authenticate a digital signature, the public official shall certify that the digital signature was affixed by the signer in the presence of the official, after having identified the signer and the validity of the public key; that the signed document reflects the signer's will; and that it is not in breach of existing law (Law No 89 of 16 February 1913). The public official's digital signature shall, for all purposes in law, complement and substitute for any seal, stamp, countersign or other distinctive mark that may be required.

With reference to the processing of electronic documents, persons in charge of the telematic transmission of data or documents created by computer-based systems shall not read and/or duplicate telematic correspondence or in any way transfer to third parties any information concerning the existence/content of such correspondence/communications or messages transmitted over telematic systems, except when such information is by its nature public and/or will be made public. Any data and/or documents transmitted by means of telematic systems will remain in the property of the sender (until delivered to the addressee).

13. Advance Analytical Tools

The Italian legal system does not have any legal provisions specifically relating to the use of analytical tools for the search, processing, review or production of ESI. However, in the context of criminal investigations involving Italian companies belonging to an international group, certain technological tools, not commonly used by in Italian proceedings, are used.

Today, more and more companies and/or groups of companies, including small and medium companies, commence internal investigations. In investigations involving several jurisdictions, the implementation of analytical tools is an advantage in terms of time and cost savings, considering the large amount of documents to be managed and the several countries involved.

Summarised below are the necessary steps that a company shall take to collect and process personal data potentially included in ESI. Personal data means any information relating to an identified or identifiable person (the 'Personal Data') in compliance with Italian applicable rules, which include Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (the General Data Protection Regulation, or GDPR) and Legislative Decree No 101/2018, which harmonises the Italian Privacy Code – Legislative Decree No 196/2003 – and other national laws with the GDPR (collectively the 'Italian Privacy Rules').

Information Notice

Prior to collection and/or processing of Personal Data, the company, acting as data controller (meaning the competent entity in determining the purposes and methods of the processing of Personal Data, including any security matters), shall inform the data subjects of the collection activities. The information notice may be provided in writing or by electronic means; if requested by the data subject, such communication may also be oral, provided that the identity of the data subject is proven by other means. The information notice shall include, inter alia:

- the main details of the company;
- contacts of the data protection officer (if any);
- the purposes and legal basis for the processing;
- the identification of the recipients of Personal Data (if any);
- a reference to the fact that the company intends to transfer Personal Data to another EU country/international organisation and the legal basis of the transfer (if this is the case);
- the period for which Personal Data will be stored or any criteria used to predict such period; and
- the rights of the data subjects, if he or she is obliged to provide Personal Data, and the possible consequences of failure to provide such data.

If the company intends to process the collected data further, for a purpose other than the one for which the data were collected, the company shall provide the data subjects with all the relevant information of the other purpose.

Consent

The data subjects shall give their consent to the processing of their Personal Data. Thus, the company shall obtain the consent of data subjects before collecting/processing their personal data. Processing without the consent is lawful only in certain cases provided by the Italian Privacy Rules and to be assessed on a case-by-case basis, including the following:

- processing is necessary for the performance of an agreement to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into an agreement;
- processing is necessary for compliance with a legal obligation to which the company is subject;
- processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the company; and

- processing is necessary for the purposes of the legitimate interests pursued by the company or by a third party, except where such interests are overridden by the interests of fundamental rights and freedoms of the data subject that require protection of personal data, in particular where the data subject is a child.

In the event that the data subject does not give his or her consent to the processing activities and none of the exceptions to the requirement of the consent applies, the company cannot process his or her Personal Data.

Data Processor
Any processing activity involving Personal Data must be performed by firms/individuals expressly appointed in writing, a so-called data processor. The data processor is the person or entity that processes Personal Data on behalf of the company. Under the Italian Privacy Rules, the agreement between the company and the data processor shall provide the subject, duration and purpose of the processing and the rights and obligations of the data controller. In particular, the agreement shall provide, among others, that the data processor:

- processes Personal Data on documented instructions from the company;
- ensures that persons authorised to process Personal Data have committed themselves to confidentiality;
- respects all the conditions set up by the Italian Privacy Rules for engaging another data processor; and
- ensures the security of processing.

In addition, for processing Personal Data in compliance with the Italian Privacy Rules, it is necessary that Personal Data is:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes, and not further processed in a manner that is incompatible with those purposes;
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;
- kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which it is processed; and
- processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, and using appropriate technical or organisational measures.

Before engaging in any investigative activities relating to electronic communications, less 'invasive' measures may be considered. In addition, in collecting and processing Personal Data, each company shall proceed in compliance with the Italian Privacy Rules, to avoid any possible sanctions as provided by the Italian Privacy Rules.

14. Production or Withholding Production of Privileged ESI

Although the Italian legal system does not provide for any specific rules relating to the protection of privileged ESI, certain documents stored electronically may be covered by legal professional privilege (*segreto professionale*) according to Italian law.

Specifically, confidentiality of written communications between lawyers and clients should be protected if the information exchange is connected to the right of defence of the client. Such legal professional privilege covers all written communications, including, as anticipated, any information stored electronically.

In the context of civil litigation, a defendant may challenge a request of disclosure by the claimant if the documents requested are covered by legal professional privilege. A party may also choose to waive legal professional privilege relating to a specific document/information if deemed appropriate.

In the context of criminal investigations, generally, all documents can be seized. However, the public prosecutor cannot carry out inspections or searches within the premises of a defence lawyer who has been appointed in a criminal proceeding, unless the defence lawyer has been indicted (Article 103 of the Italian Procedural Criminal Code). In addition, the public prosecutor cannot seize any documents at the lawyer's premises relating to the defence's strategy, the defence's investigations and any correspondence with the client.

All documents can potentially be seized by the Italian Competition Authority (ICA). Among other powers, the ICA can (i) conduct inspections within the investigated company and (ii) take copies of books and/or business records. Such powers are subject to various limitations (eg, the protection of confidentiality). In addition, because of legal professional privilege, the ICA cannot examine certain communications between a company and its lawyers.

Legal professional privilege is limited to the communications between the defendant and his external lawyers, and, thus, does not cover the communications between the client and their in-house lawyer.

15. Privacy Statutes & Rules or Regulations

As previously explained, the Italian legal framework does not provide any specific provisions relating to the disclosure/discovery of ESI. However, it is possible to consider the legal framework that shall apply to the disclosure of sensitive data – potentially included in ESI – in the context of internal criminal investigation. In addition to the privacy regulations

mentioned in **13 Advance Analytical Tools**, there are other rules and principles that should be taken into consideration when dealing with the disclosure of sensitive data and documents.

Corporate Governance
Several issues may arise when information relating to the developments or outcomes of the investigation are disclosed – or not – to the company's functions or bodies (eg, HR, managing body, board of statutory auditors and internal counsel) and/or to the parent company and/or other affiliates or subsidiaries (eg, information flows not in compliance with the internal procedure and lack of transparency).

Labour Law
The interest of the company (employer) to confidentiality, which is also needed to ensure the effectiveness of the investigative activities, shall be balanced with the right of defence of the employees as provided under labour law.

According to Italian employment law, control over the employee's activity is generally forbidden, meaning that the employer could not adopt any instruments (including technical tools) to control the working activity of the employees, even if adopted for other reasons (Article 4 of Law No 300/1970 – the Italian Workers' Statute of Rights).

On September 2015, the above-mentioned Article 4 was amended and today employers can process and use all information obtained from any devices given to employees for working activity (eg, laptops or mobile phones). The company/employer can use the information obtained from these devices for any purpose relating to the employment relationship (eg, for evaluating the employee or for disciplinary issues), by informing the employee in advance of such activity and in compliance with Italian applicable data privacy rules. Therefore, companies should implement new policies in which they fully clarify how the work equipment will be used, including what can be considered as work equipment.

Italian Legislative Decree 231/2001
Internal investigations are crucial for a company's defence if the allegations trigger any corporate liability. Specifically, under Italian Legislative Decree No 231 of 8 June 2001, a company may incur 'administrative' liability – actually, quasi-criminal – in relation to specific categories of crimes (which include, public corruption, private corruption, crimes related to health and safety law matters, crimes against the environment, corporate crimes and false disclosures in corporate notices, and criminal conspiracy) committed by directors, officers or employees of the company, in the interest or to the benefit of the company. A company may also be held liable under Decree 231 if a person who is not formally a director, officer or employee is de facto acting in such capacity.

Decree 231 exempts the company from liability if it can be demonstrated that, before the crime was committed, the company adopted and effectively implemented an adequate *Modello di Organizzazione, Gestione e Controllo ai sensi del Decreto Legislativo 8 giugno 2001, n. 231* (the '231 Model') and appointed a body vested with autonomy of initiative and control powers to supervise the implementation of the 231 Model (a so-called Supervisory Body). The Italian system provides that, in order to implement an adequate 231 Model for the purposes of Decree 231, companies are required to:

- identify the activities in the context of which offences may be committed (risk analysis);
- establish appropriate procedures for the purposes of passing and implementing decisions relating to the prevention of crimes;
- set forth adequate rules for the management of financial resources to prevent crimes from being committed;
- provide for reporting duties to be complied with by the Supervisory Body;
- introduce an appropriate disciplinary system for the purpose of sanctioning cases of failure to comply with provisions of the 231 Model; and
- introduce a whistle-blowing channels.

Although the adoption and implementation of a 231 Model is not mandatory by law, in practice, Italian companies that demonstrate that they have in place an effective compliance programme to prevent the commission of crimes and to monitor the risk areas in which they operate may avoid or reduce potential liability under Decree 231 (provided that some further conditions are met). Therefore, companies have a strong incentive to adopt the 231 Model and internal investigations are often tools to find, among others, potential defects in the 231 Model and adopt appropriate remedial actions.

Whistle-blowing
At the end of 2017, Italy introduced a new legislation on whistle-blowing according to which public/private sector employees shall be protected if they report illegal practices within their company. Specifically, employees are protected by specific rules that safeguard them from dismissal and from any form of discrimination or disciplinary action as a consequence of having signalled to the authorities any unlawful practices. It is worth mentioning that there is no clear definition of what makes a disclosure relevant according to this specific legislation, provided that employees may not make unfounded allegations that could damage the reputation of the company/employer. In accordance with general principles of law, any such disclosure must be based on specific information and supported by the relevant evidence. The law does not provide for a specific procedure for making such a 'disclosure': employees shall be able to report any unlawful practice; however, each company can adopt its internal specific policy. It is worth mentioning that there

is an increasing awareness that the implementation of an internal policy reduces the risk of reputational damage for the employer; by managing the raised concern internally. In the event of an unfair dismissal of an employee relating to a protected disclosure, an individual can, among other rights, return to his or her job and/or obtain the payment of related damages.

16. Transfer of ESI Outside Jurisdictional Boundaries

The main rules introducing constraints to the transfer of ESI to foreign jurisdiction are set forth in the privacy regulation.

Italian privacy rules are contained in Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and in Legislative Decree No 101/2018, which harmonises the Italian Privacy Code – Legislative Decree No 196/2003 – and other national laws with the GDPR (collectively, the 'Italian Privacy Rules'). The Italian Privacy Rules apply when the transfer of ESI contains personal data (ie, any information relating to an identified or identifiable person).

Under the Italian Privacy Rules, transfer among European countries is allowed as far as all the conditions of lawful and licit processing as detailed in the rules are met.

A transfer of personal data to a country outside the EU or an international organisation might occur only if more stringent conditions are met. These include if the EC has decided that the third country, the relevant territory, or the international organisation ensures an adequate level of protection. In this case, the transfer shall not require any specific authorisation.

Specifically, the non-EU entities receiving Personal Data are considered to ensure an adequate level of protection if they are certified in the context of the Privacy Shield Framework for the transfer of data between the EU and the USA, or if they have been authorised by means of the EC Model Clauses approved under Directive 95/46/EC or if they have been authorised in compliance with the other requirements provided by the Italian Privacy Rules; for instance, through the so-called binding corporate rules.

When assessing the adequacy of the level of protection, the EC shall take into consideration, among others, the following elements: relevant legislation, respect for human rights and fundamental freedoms, defence, national security and criminal law, access of public authorities to personal data, as well as data protection rules and security measures.

In addition, the GDPR provides for "derogations for specific situation." Specifically, in the absence of an 'adequacy decision' or of appropriate safeguards mentioned above, including binding corporate rules, a transfer of personal data to a third country or an international organisation might occur if certain specific conditions are met. In particular, among others:

- if the data subject has given his or her explicit and informed consent to the transfer of his or her personal data, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for establishing or defending a legal claim;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; or
- the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent. The circumstances listed above are applied by the Italian Data protection authority (*garante*) in a restricted way.

Additional restrictions to the transfer may be contained in special rules applicable to certain sectors (eg, industrial sector, banking secrecy).

Paul Hastings (Europe) LLP
Via Rovello, 1
20121 Milan,
Italy

PAUL HASTINGS

Tel: +39 02 30414 000
Fax: +39 02 30414 005
Email: marilenahyeraci@paulhastings.com
Web: www.paulhastings.com/office/milan