THE EUROPEAN, MIDDLE EASTERN AND AFRICAN INVESTIGATIONS REVIEW 2016

Published by Global Investigations Review in association with:

Paul Hastings

GIR

Global Investigations Review

www.globalinvestigationsreview.com

Italy

Bruno Cova and Francesca Petronio
Paul Hastings

Corporate internal investigations were almost unheard of in Italy until the adoption of Legislative Decree No. 231 of 8 June 2001 (Decree 231), which introduced the 'quasi-criminal' liability of corporations for certain crimes committed in their interest or to their advantage by their directors, managers, employees or agents. A company can, however, avoid such liability if it has adopted and implemented an effective compliance programme (or 'organisational model') for the prevention of the relevant crime.

Following the implementation of Decree 231 various criminal proceedings were brought against Italian and foreign companies. Gradually, many companies, especially those belonging to multinational groups, adopted an organisational model according to Decree 231 and started conducting internal investigations as an instrument of risk management.

The absence in Italy of a duty to self-report also contributed to making the internal investigation a useful instrument to detect and prevent or interrupt improper behaviours, which could otherwise expose the company to criminal proceedings and its consequences.

The reform of Italian company law of 2004, and other legislative measures, particularly in regulated industry sectors such as banking, insurance and listed companies, attributed to company directors an increasing level of responsibility for the internal control system, encompassing among their duties the adoption of adequate organisational, administrative and accounting structures (article 2381 of the Civil Code). Company directors also have the duty to act in an informed manner (article 2381 of the Civil Code) and are held liable if, aware of damaging circumstances, they do not intervene in order to prevent such circumstances or, at least, to minimise or avoid damaging consequences (article 2392 of the Civil Code).

In this scenario, internal investigations have come to represent a fundamental element of a robust internal control system capable of providing directors with the information they need to act in an informed manner and to take appropriate and timely measures in case of improper behaviour.

Immediately after the adoption of Decree 231, public prosecutors took a sceptical view of companies conducting internal investigations since they were afraid that this could impede their investigative activity. More recently, prosecutors have realised that internal investigations can help in expediting proceedings, save costs and, at the same time, make companies under investigation more conscientious and their management more responsible as to the outcome of the criminal proceedings.

The liability of legal entities pursuant to Decree 231

Decree 231 has been partly modelled on the US Sentencing Guidelines for Organizations and was passed to meet the requirements of the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions of 1997.

Under Decree 231, in particular, companies may be directly liable when individuals (i) who hold representative, administrative or executive positions in the company or in any of its branches granted with financial and organisational autonomy, or who de facto manage it, or (ii) who are subject to the direction and supervision of one of the persons under (i), commit one or more crimes listed in Decree 231 in the interest or to the advantage of the company, unless the company adopted and effectively implemented a suitable organisational model before the crime was committed.

In addition to the quasi-criminal liability pursuant to Decree 231, the company can also be held liable for the damages suffered by the victims of the crimes committed by its employees in the context and by virtue of their working relationship pursuant to the vicarious liability principle (article 2049 of the Civil Code).

Offences contemplated by Decree 231

Decree 231 contemplates an imperative list of crimes that can trigger the liability of the corporation.[1] The list has been subject to many legislative amendments which have considerably expanded it.

The main offences may be grouped as follows:

- Crimes against the Public Administration, which include undue receipt of public funds, fraud to the detriment of the state or other public entities, corruption and extortion.[2]
- Corporate crimes, which include false disclosures in corporate notices, prospectuses and auditors' reports, impeding controls, preventing regulatory authorities from carrying out their functions and private corruption.
- Money laundering, self-money laundering and other related crimes.
- Crimes against trade and industry, which include fraud against the national industries, fraud in trade practices, sale and commerce of counterfeited products.
- Crimes related to copyright violations, which include illegal sale, reproduction, or any public or commercial distribution of any product protected by copyright.
- Crimes against the environment.[3]
- Homicide and serious injuries deriving from the violation of the rules protecting health and safety in the workplace.
- Cybercrimes.[4]
- Market abuse, insider trading and market manipulation.
- Cross-border crimes under Italian Law No. 146 of 2006.
- Crimes related to the use and/or the exploitation of irregular foreign workers and crimes against individual freedoms.
- Crimes aimed at terrorism and reversal of the democratic system.
- Crimes related to organised crime.

Sanctions

If a company is found liable under Decree 231, it may be subject to a combination of sanctions including a fine of up to €1.5 million (in case of a plurality of crimes, up to €4.5 million), the seizure of the profits resulting from the crime, the publication of the court's decision, and disqualifying sanctions ('blacklisting').

Disqualifying sanctions may have a considerable impact on the business of the company as they include, among other

things, disqualification from performing part or all of its business, suspension or revocation of authorisations, permits, licences or concessions, functional in the commission of the crime, prohibition from negotiating with the Public Administration, exclusion from benefits, loans, contributions, as well as revocation of those that have already been granted; and prohibition of advertising goods or services offered by the corporation. Finally, it must be considered that disqualifying sanctions in some instances can be applied also as precautionary measures.

Exemptions from liability

Decree 231 provides that a company can be exonerated from liability if it proves that the individuals who committed the crime acted solely in their own interest or on behalf of third parties and not in the interest of the company, or that the company has adopted and implemented effective internal control systems for the purposes of preventing the criminal offences at hand, before any offence was committed, and has set up of a supervisory body properly vested with independent initiative and inspection powers.

The implementation of an organisational model after the commission of the relevant crime cannot exempt the company from liability, but it can grant a reduction of the applicable sanctions and avoid the application of debarment. The ex post implementation of an effective organisational model can also exclude the risk of reoccurrence of the crime and therefore avoid the application of protective interim measures.

The decision to investigate

The decision to start an investigation can be driven by a variety of factors in addition to the case in which a criminal proceeding against the company had been commenced for a Decree 231 related offence.

As anticipated, a robust internal control system will require the company and its management and control bodies to react and initiate an investigation, for example, in case of whistleblower allegations, of red flags emerging in the context of M&A transactions or an audit, press rumors, or request of information by regulators.

When the internal investigation is started in the absence of an ongoing criminal investigation the management may want to commence an investigation with a view to interrupting any wrongdoing and preventing any regulatory action, demonstrating that the company is able to react and that the internal control system works properly; additional drivers to the decision to investigate include the willingness to take disciplinary or other actions against wrongdoers, limit damages and losses, and identify any weakness in the internal control system.

An important factor to consider in this context is the absence for private entities and individuals of a duty to report to public authorities any crime discovered in the context of an internal investigation.

The only exception to this principle regards the board of statutory auditors of listed companies who are under an obligation (article 149 of Legislative Decree No. 58 of 24 February 1998) to notify Consob (the National Commission for Companies and Stock Exchange) of any irregularities found in the context of their supervisory activity.

In deciding whether to self-report, notwithstanding the absence of any duty to do so, companies will also need to consider that prosecutors have a mandatory duty to start a criminal investigation in the event they receive a notice of a crime and that there is no instrument similar to the deferred prosecution agreement available to the corporations as an incentive to self-reporting.

When a criminal investigation into the company or its managers or employees is commenced by a prosecutor, starting an internal investigation can represent a remedial action to be shown to the proceeding authority in an effort to mitigate sanctions and avoid disqualifying ones (also as precautionary measures) and defend the company's reputation. Investigations can also be useful to gather elements and information that can be used in the defence in the criminal proceeding and any related damages claims.

In these cases, the company will need to appoint an external counsel to defend and represent the company in the criminal investigation and to coordinate with the public prosecutor so that the proceeding authority may not be induced to think that someone is interfering with the criminal proceeding.

In an official circular of March 2012, the Tax Police ('Guardia di Finanza', which has broad responsibilities for investigating white-collar crimes) underlined the key role of internal investigations as a pretrial instrument of defence for companies, evidencing that through internal investigations companies can find crucial elements which could be used as evidence during the judicial proceedings.

Defensive investigations pursuant to the Code of Criminal Procedure

The Code of Criminal Procedure expressly disciplines the investigation carried out by external attorneys and consultants (including detective agencies) for the purpose of conducting pretrial internal investigations (article 391-bis of the Code of Criminal Procedure et seq).

Attorneys specifically appointed by the clients – as well as authorised investigators and consultants – have the possibility to collect evidence through interviews of individuals, direct access to relevant locations and, also, making a specific request for relevant documents held by public entities.

The persons who are requested to be interviewed may at any time exercise their right to refuse to answer and, in any case, the questioning must be suspended whenever clues of guilt against the interviewed come out.

Additional cautions are raised for special situations: for example, people involved in the same (or in a related) proceeding must be assisted by their lawyer during the questioning; also, in case of questioning of a detainee, the previous authorisation of the judge is needed.

As per the access to relevant locations, the Code of Criminal Procedure sets some restrictions: the access to private places needs the consent of the owner and, in case of denial, the judge must authorise it. In any case, access to dwellings may take place only if it is necessary to obtain traces or other material evidence of the crime.

Once the investigation is completed, the attorney may, at any time during the judicial investigations and until the preliminary hearing, disclose to the judge the outcome of his or her defensive investigations: such material is filed in the defence records and may be taken into account by the judge in the decision of the matter.

Anyway, lawyers are not obliged to disclose to the public authorities any eventual crime found during their appointment.

Key constraints on investigations

Most of the investigative activities to be carried out may interfere (and normally do interfere) with the rights of the employees. Compliance with data protection laws and labour laws is therefore key to avoid the outcome of the investigation being jeopardised by violations of those statutes. Foreign companies conducting internal investigations on their Italian subsidiaries should be particularly alert to the peculiarities of Italian law, to avoid unwittingly committing irregularities that can often be more serious than those originally investigated.

In general terms, when conducting internal investigations, a balance must be found between the right of the employer to protect the company's assets and to interrupt improper behaviour and the right of the employee under investigation to have his or her constitutional privacy and dignity rights protected.

Article 8 of Law No. 300 of 20 May 1970 (the Workers' Statute) prohibits the employer from investigating employees' opinions related to politics, religion, trade unions and personal life; article 4 of the Workers' Statute, as recently reformed by Legislative Decree No. 151 of 14 September 2015, prohibits remote surveillance or monitoring of workers by 'audio-visual equipment' or 'other equipment' (referred to as 'distant monitoring') if the ultimate scope is to monitor the employees' performances.

Distant monitoring in the workplace is allowed only in case of organisational, business or security needs and only if the employer reaches an agreement with the workers' representatives; or in the lack of such agreement, if the distant monitoring tools are approved by the Labour Inspectorate.

Distant monitoring, including through hidden instruments, is allowed if aimed at finding unlawful behaviour of the employee, other than a mere breach of job performance.[5]

Exceptions to these principles have been recently introduced for control on the instruments used by the employees for working (including computers, tablets, mobile phones).

In any case the information gathered through those instruments must be used fairly in connection with the working relationship.

Conducting an internal investigation implies the processing of personal data and requires compliance with data protection laws. Personal data must, among other things, be processed lawfully and fairly and collected for specific, explicit and legitimate purposes. The processing must be necessary and not excessive in relation to the purposes of the collection, and data can be stored for no longer than is necessary for the purposes for which the data were initially collected.

According to the 2007 Guidelines of the Privacy Authority, companies should introduce IT policies approved by trade unions that allow for controls of internet files and emails. The policy must inform employees that the employer may perform controls in the context of investigations.

The processing of personal data is generally allowed only if there is a policy in place or if the individual whose data are subject to processing gives his or her express written consent (article 23 of Legislative Decree No. 196 of 30 June 2003 (the Data Protection Code)) and the data subject receives specific information in connection with that specific data processing (article 13) in advance.

Controls on an employee's emails and files can be conducted even in the absence of a specific policy and consent if the processing is aimed at establishing or defending a legal claim, or conducting defensive investigations, provided that the data are processed exclusively for said purposes and processing is made in compliance with the principles set forth by the law.

Similarly, the information to the employee could also be omitted in the event it could jeopardise the outcome of the investigation.

Data retrieved in violation of the data protection laws cannot be legitimately used and the unlawful processor (including the company itself) could be exposed to severe sanctions, including criminal sanctions. Data processing without the due consent could constitute a crime under article 167 of the Data Protection Code; violation of correspondence could also constitute a crime under article 616 of the Criminal Code.

In addition to the criminal sanctions, the employee whose data have been processed unlawfully may bring a civil action seeking the damages suffered as a consequence of the unlawful processing of his or her personal data. Lastly, data retrieved in violation of the law cannot be used as evidence (eg, in a case of unfair dismissal) and must be destroyed.

The Privacy Authority, through decision No. 60 of 6 November 2008 approved a code of conduct with the principles that must be respected in processing personal data when carrying out defence investigations and, more in general, throughout the activities of defence in a judicial claim; in particular, the lawyer conducting the investigation shall respect the data subjects' rights, freedom and dignity, according to the principles of purpose limitation, data minimisation and proportionality, and the quality and amount of information to be processed shall have to be taken into account along with the possible risks.

If data is processed to exercise the right of defence before a judicial authority, this may take place prior to instituting the relevant proceeding on condition that the data in question is strictly functional to exercising the right of defence and the principles of proportionality, relevance, completeness, and proportionality are complied with by having regard to the defence purposes.

Legal privilege

While conducting internal investigations in Italy one must consider that Italian law does not provide for the privilege of documents in the same manner contemplated by the attorney-client privilege doctrine of the US or other common law countries. The protection of confidentiality between lawyers and their clients (the 'professional secrecy' doctrine) is limited in scope and rather than protecting certain documents according to their origin or creation, the law sets forth specific procedures and precautions to be adopted for gathering and using the documentation exchanged between a law firm and its clients.

It is a general duty of the lawyer to maintain secrecy on his or her activities and on all the information received by the client or known depending on the defensive mandate.

A lawyer can refuse to deliver documents or any other object provided by the client by objecting to professional secrecy during investigations carried out by judicial or regulatory authorities. In such cases, a judge has the authority to verify whether there are any grounds to oppose the professional secrecy.

The protection only applies to communications between the defending counsel duly appointed and the indicted or investigated person. If the defendant is a company, the legal privilege only applies to communications with the person who has the power to represent the company. As a consequence, if the relevant communications with the defence lawyer are handled by other persons, the communications would be considered as no longer protected by professional secrecy and if they are forwarded to other persons no professional secrecy protection will apply as well.

The protections listed above apply only to lawyers who are members of the Italian bar, and not to in-house counsel, nor to foreign lawyers.

Use of detective agencies

The Privacy Authority's decision No. 60 of 2008 sets forth some guidelines for detectives to be involved in intenal investigations aimed at protecting data in the context of investigations.

Detective agencies must receive from the employer or outside counsel a specific written mandate which specifies the legal claim the employer wants to establish or defend, the purposes of the investigation, the reasons and the elements that justify the investigation,[6]

the duration of the investigation, the names of the detectives, the obligation to report periodically, and the right of the detective to keep the data.

Structuring the investigation

There are some preliminary activities that can be organised to be ready and ensure compliance in case the urgent need to start an investigation arises.

Those measures include the introduction of a specific policy to deal with some of the most controversial aspects of an internal investigation including the involvement of external counsel, confidentiality, the appointment of detective agencies and data processing.

To make data processing lawful, policies related to emails, laptop, and internet use can be adopted and agreed with the works councils.

Policies regarding the use of IT resources should specify the permitted use of email and the internet by employees, liability deriving from misuse, duty of secrecy, security measures, password management, and the possibility to deny the access to websites unrelated to the scope of work.

Additional tests that can be done in advance include a review of the delegation of powers to verify that disciplinary and data privacy powers are attributed correctly, and a review of whistleblowing schemes.

Conducting the investigation

When an internal investigation starts, the first thing to be done is to determine the scope of the work and objectives. The internal investigation may help the company to understand, for example, how many wrongdoers and wrongdoings are involved; if external consultants, clients or business partners are exposed; how many jurisdictions are involved; if wrongdoing is systemic; if it is extended to other group functions or companies; if it is still occurring, which part of the company's business is affected; if the control systems are adequate; and if the company's controlling bodies or auditors have exercised effective control.

A detailed investigation plan is a good instrument to manage the investigation and identify and deal with the key constraints and avoid any pitfalls. The plan shall consider that a strategic key to success is operating always in compliance with applicable laws and to preserve legal privilege, and collecting proper evidence. The plan should define what kind of investigation shall be carried out, whether to use a step-by-step approach, if and when to conduct interviews, or whether to start a forensic audit or an e-discovery.

In this context, the plan shall also address preliminary activity to be carried out to ensure compliance, such as any appointment of data processors if data processing is involved, their engagement through external lawyers to preserve privilege, the appointment of detectives, and the use of any certified tools to grant security of the data retrieved.

Corporate governance issues should be addressed at an early stage, including any need to convene shareholders' or board of directors' meetings and any precautionary resolution to be adopted (eg, revocation of powers of managers potentially involved, suspension of business partners or contracts with third parties, adopting measures to guarantee an unadulterated flow of information to the directors).

The investigation will strive to understand at a preliminary stage what the potential consequences are of the wrongdoing identified (regulatory action, criminal liability, accounting and tax issues, damages claims), the losses suffered, and how the company can mitigate the damages and prevent further wrongdoing.

The plan will need to cover immediate actions to collect evidence, safeguard information, including immediate action to preserve documents (eg, through the issuance of document retention policies or freeze notices, hard disk imaging, and securing hard copy documents).

Aspects that should be always addressed include confidentiality and the protection of the individuals under investigation and of the whistleblower, if any. Immediateness of analysis and of the reaction is key and in this regard, legal issues must be analysed as soon as they arise to avoid jeopardising the possibility of remedial action. A constant flow of information will help coordination and prevent pitfalls.

Interviews

There are no specific obligations of employees and managers to be interviewed other than a general duty of cooperation of the employee and possibly a specific provision in the code of ethics of the company that requires employees to cooperate and support during internal investigations.

Interviews constitute a delicate moment in the context of an internal investigation as they should be only aimed at fact gathering; potential challenges to employees may not be raised during the interview as they must follow the specific procedure set forth by labour law. As soon as the employer detects any employee's improper conduct and violation of his or her labour law duties a written notice must be addressed to the employee identifying the challenges. The employee then has five days to provide his or her justification in writing. Only after these steps may the employer decide to apply disciplinary measures (including dismissal) if the justifications given by the employee are considered inadequate.

Email review

An essential prerequisite to avoid privacy and labour law pitfalls in email screening is the implementation of a specific policy approved by the works council on use of electronic devices and controls allowed by the employer.

In the absence of a specific policy the rules on the need for obtaining the employee's consent and to provide information in advance shall be respected, unless the exceptions under applicable data protection law can be applied. Moreover, the controls on emails should always follow the principles of necessity, proportionality and adequacy, so that the employer may conduct email review only if it is necessary in the context of the investigation and there is no less intrusive way to obtain the same result. Email review must be conducted through the use of keyword searches to minimise the risk of collecting unnecessary data.

A different level of caution must be adopted depending on the level of involvement in the wrongdoings of the employee whose emails are subject to review (in compliance with the principles of necessity and proportionality).

Access to documents

The employee must provide access to letters, files and documents that are business related and that are requested in the context of the investigation. The existence of a policy on the conservation of files may help in obtaining quick and complete access to the documents needed and may also be important in case of investigations by public authority. Similarly the issuance of a document retention or freezing notice at the beginning of the investigation may help in preventing employees from destroying documents and jeopardising the result of the investigation.

Use of the information in the investigation

Data protection and the rights of the employees must also be taken into consideration when the investigation is over and the company may be willing to share its outcome and findings with different subjects. If those findings contain employees' personal data the mandatory privacy requirements of obtaining the employee's consent (if exceptions are not applicable) and providing him or her an information notice apply.

This is particularly relevant in case of multinational groups where the third party accessing the data gathered from the investigation may be based abroad. In this case the data protection rules on the transfer of the data to third countries must be followed.

Closure of the investigation and remedial actions

The outcome of the investigation and its findings shall be subject to a thorough analysis to understand what measures may be adopted to interrupt wrongdoing, prevent any further violations and correct any weaknesses in the internal control system.

Specific disciplinary actions vis-à-vis the employees or contractual remedies against business partners may be taken, including actions for damages.

In addition, a company may want to evaluate whether to disclose the outcome of the investigation to any regulator, provided that no duty to self-report exists for private entities in Italy.

Notes

1 See article 24 et seq, Decree 231.

2 The Italian system provides further measures against public corruption, which include the National Anti-Corruption Authority, with supervising and controlling powers; whistleblowing mechanisms; and extraordinary anti-corruption measures in the context of participating in public tenders (Law No. 190 of 2012, and Law No. 114 of 2014).

3 The crimes from (n) to (s) have been recently introduced by Law No. 68 of 2015.

4 These crimes have a wide application and are applicable to any illegal access to IT systems processing data (including, for example, the energy platforms of the Gestore dei Mercati Energetici SpA).

5 Supreme Court, 27 May 2015. Distance controls are permitted in case of wrongdoings of the employee in order to protect the assets' integrity (Supreme Court, 1 June 2010).

6 Supreme Court, 31 October 2013; Supreme Court, 8 June 2011; Supreme Court, 14 February 2011; Court of Milan, 18 April 2009.

Bruno Cova
Paul Hastings

Bruno Cova is partner of global law firm Paul Hastings and chair of its Milan office. He focuses his practice on mergers and acquisitions, restructurings, securities law and corporate governance and corporate crises. In the field of corporate governance, he advises general counsel and boards of directors on governance reforms, legal risks and internal controls, regulatory and internal investigations.

Mr Cova was general counsel of Eni E&P and Fiat Group and chief compliance officer of the European Bank for Reconstruction and Development. Immediately before joining Paul Hastings he served as chief counsel to the commissioner appointed by the Italian government to investigate Europe's largest financial fraud at Parmalat.

He is also an officer of the International Bar Association Anti-corruption Committee and a member of the troika of experts advising the Corporate Governance Committee of Borsa Italiana on governance reforms.

Francesca Petronio
Paul Hastings

Francesca Petronio is a partner in the litigation practice of Paul Hastings and is based in the firm's Milan office. Ms Petronio has extensive experience in litigation, domestic and international arbitration, bankruptcy, corporate and commercial litigation matters, as well as the management of pre-litigation situations. She has extensive experience in dealing with compliance programs-related issues, white-collar crimes, data privacy issues providing assistance to domestic and international clients in internal investigations.

Mrs Petronio was named among the 100 remarkable women in investigations from around the world by *Global Investigation Review* in 2015.

She is also an officer of the International Bar Association Anti-corruption Committee where she chairs the Sub-committee on double jeopardy.

PAUL
HASTINGS

Via Rovello, 1
20121 Milan
Italy
Tel: +39 02 30 414 000
Fax: +39 02 30 414 005

Bruno Cova
brunocova@paulhastings.com

Francesca Petronio
francescapetronio@paulhastings.com

www.paulhastings.com

Paul Hastings is a leading global law firm with offices throughout Asia, Europe, South America and the United States. Global investigations are one of Paul Hastings' main practice areas. We represent boards of directors, general counsel and chief compliance officers in identifying and assessing risks, devising internal control systems and compliance programmes, conducting internal investigations, defending corporations in the context of enforcement actions and taking remedial actions such as disciplinary measures against wrongdoers, reinforcing internal controls and bringing damages claims. Our clients include industrial companies and financial institutions. Our global investigations team operates from multiple countries and has an unparalleled expertise in handling multi-jurisdictional investigations in several countries.

Strategic Research Sponsor of the
ABA Section of International Law

Law
Business
Research

THE QUEEN'S AWARDS
FOR ENTERPRISE:
2012

ISSN 2059-271X