THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW

THIRD EDITION

Editor
Jennifer Mott Williams

THE LAWREVIEWS

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW

THIRD EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in May 2021
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Jennifer Mott Williams

THE LAWREVIEWS

PUBLISHER
Clare Bolton

HEAD OF BUSINESS DEVELOPMENT
Nick Barette

TEAM LEADERS
Jack Bagnall, Joel Woods

BUSINESS DEVELOPMENT MANAGERS
Katie Hodgetts, Rebecca Mogridge

BUSINESS DEVELOPMENT EXECUTIVE
Olivia Budd

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Tommy Lawson

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Helen Sou

SUBEDITOR
Anne Borthwick

CHIEF EXECUTIVE OFFICER
Nick Brailey

Published in the United Kingdom
by Law Business Research Ltd, London
Meridian House, 34–35 Farringdon Street, London, EC4A 4HL, UK

www.TheLawReviews.co.uk

ISBN 978-1-83862-772-0

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following for their assistance throughout the preparation of this book:

BOMCHIL

DEMAREST ADVOGADOS

FÉRAL-SCHUHL / SAINTE-MARIE

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP J

MORGAN, LEWIS & BOCKIUS LLP

PETILLION

TMI ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

CONTENTS

PREFACE

Virtually unheard of 20 years ago, increasing data volumes and ever-changing technologies have resulted in e-discovery and information governance exploding onto the legal scene. Corporations face a wide array of overlapping and competing e-discovery and information-governance laws and regulations impacting the use, retention and disposition of electronically stored information (ESI). This third edition of *The e-Discovery and Information Governance Law Review* provides a general overview of e-discovery and information-governance obligations in key jurisdictions around the world.

E-discovery seeks the disclosure of ESI to opposing parties, regulators, governing authorities and judiciaries. It is a complex issue that requires a strategic and thoughtful response, with greater consideration given to newer technologies, such as mobile applications, file-sharing sites and collaborative tools, utilised by an increased remote workforce as a result of the covid-19 pandemic. Although e-discovery is common in some countries, such as the United States, it remains a foreign – sometimes unheard of – concept in other jurisdictions throughout the world.

In contrast to disclosure obligations, many jurisdictions seek to protect their citizens from cross-border data flows and the disclosure of information abroad. Data-protection regulations continue to evolve in those jurisdictions that have them, and an increasing number of jurisdictions that did not previously have data-protection regulations are implementing them. Thus, global corporations may face unique challenges when international data is sought in e-discovery: failure to comply with e-discovery obligations could result in sanctions against an organisation, while the corresponding disclosure of ESI and failure to comply with data-protection laws could result in the imposition of fines or criminal prosecution.

Recent global events have further complicated data privacy. The covid-19 pandemic is causing many jurisdictions to amend their data privacy laws in pursuit of the common good. However, whether jurisdictions will extend those laws beyond the end of the pandemic and what will happen to data collected during the pandemic has yet to be determined. Further complications to data privacy may arise as more jurisdictions debate potential vaccine passport mobile applications.

Information governance is likewise an intricate issue, involving the organisation and the maintenance, use and disposition of information in light of business goals, as well as complex legal and regulatory obligations. Effective information governance provides an organisation with an opportunity to control ever-expanding data volumes as well as newer technologies and forms of ESI. It also provides corporations with knowledge and insight into their own data assets so that they know what information they have, where it is kept and how it is being used.

Information governance further includes having processes in place for handling sensitive information that may be governed by various data-protection laws or other regulations. With more employees working remotely throughout the world, the covid-19 pandemic has pushed many businesses to reassess their technological offerings and information-governance policies to adapt to the way employees now conduct business.

E-discovery and information governance intersect whenever ESI is implicated in a litigation or regulatory investigation. A critical element of any information governance programme is a defensible, repeatable e-discovery plan that includes processes and procedures for handling ESI in the face of an anticipated litigation or government investigation implicating e-discovery. Because an effective programme of this kind keeps only those materials for which an organisation has a business need or legal obligation, data volumes are limited, along with the corresponding risks and costs associated with e-discovery.

While this book provides a basic overview of issues and highlights best practices in each jurisdiction covered, given the complex and ever-evolving nature of e-discovery and information governance laws, we strongly encourage you to reach out to counsel for assistance with any issues you may encounter.

We would like to thank all the contributors for generously lending their time and expertise to help create this third edition of *The e-Discovery and Information Governance Law Review*. We would also like to thank the *Law Reviews* team, without whom this work would not have been possible.

Jennifer Mott Williams
Morgan, Lewis & Bockius LLP
Houston
April 2021

Chapter 8

SPAIN

Enrique Rodríguez Celada, Sara Sanz Castillo and Reyes Bermejo Bosch[1]

I OVERVIEW

Unlike those of many other countries, the Spanish legal system does not regulate discovery in the sense of a process involving the obligation to preserve information in light of a reasonable expectation of litigation and disclose that information at the request of a third party in the context of potential or actual court proceedings. Spanish legislation does not even set out a discovery (or similar) process to preserve and disclose a broad range of information or data.

Spain filed reservations under Article 23 of the 1970 Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters to expressly exclude the execution of letters of request issued for the purpose of obtaining pretrial discovery of documents, which indicates the absence of a discovery culture in the country.

Contrary to the uniform and general discovery process in place in other jurisdictions, under Spanish law, data preservation obligations result from sectoral regulation, and their scope is limited to specific documents and content. Data disclosure obligations arising from a third party's request can only result from a judicial order issued by a court within litigation proceedings (meeting the requirements applicable in each jurisdiction) and, exceptionally, in the case of criminal proceedings, from dawn raids and document seizures ordered by a criminal court.[2]

These preservation and disclosure obligations are strengthened by the consequences attached in the event of breaches, which range from procedural consequences (i.e., reassessment of evidence) to administrative and even criminal sanctions, depending on the circumstances of the specific infringement.

In addition to the absence of a discovery process and governing framework, sectoral laws regarding data collection and data disclosure do not refer to electronically stored information (ESI) expressly (except for criminal procedure regulations). However, it is assumed that this category of information falls within the scope of terms such as data and documents, which are most commonly used by the legislature.

---

1 Enrique Rodríguez Celada is counsel, Sara Sanz Castillo is a senior associate and Reyes Bermejo Bosch is a managing associate at Uría Menéndez Abogados, SLP.

2 Pursuant to Article 261(5) of the Spanish Civil Procedural Law, dawn raids can also be carried out in civil proceedings, at the pretrial stage, in the event that a prior request of data was disregarded and that the requested information was necessary to obtain a medical file or determine the members of a group of consumers or users affected by a certain product, or in the context of civil proceedings resulting from the infringement of industrial or intellectual rights to the extent set out by Article 250(1)(7) of the Spanish Civil Procedural Law.

As a result of having no discovery process, cases in which courts and other parties have had to deal with a vast amount of data have been rare until very recently. Thus, digital forensics and legal professional privilege have not developed to the same extent as seen in other jurisdictions. However, this has started to change, as expansive information requests, new technologies and internal investigations are becoming more commonplace.

II YEAR IN REVIEW

The laws relating to data preservation and disclosure obligations, especially the former, are in constant development. Consequently, so are the provisions.

European regulations play a key role in this development, given that recent changes in matters relating to e-discovery originate from those regulations. In this regard, in November 2020 the European Data Protection Board adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Steps have also been taken to transpose the Whistle-blower Directive[3] into Spanish law (i.e., after the publication of the Directive on 26 November 2019, the public consultation stage followed and has already finalised). However, the terms of the new regulation to be passed to implement this Directive are not yet clear.

Important European initiatives were announced in 2019 that will lead to amendments of the Spanish legislation and procedures regarding e-discovery in the years to come (e.g., the European Commission's proposals to start international negotiations on cross-border access to electronic evidence[4] and for the harmonisation of procedures to be followed within the European Union for the gathering and production of e-evidence[5]). No significant developments in this regard took place during 2020.

In terms of domestic developments, a new Lawyers' General Statute has been approved. Although the final wording of the new law has not been officially published yet, it seems that it will extend legal privilege to in-house lawyers, thus limiting the scope of disclosure proceedings (see Section V).

Additional limitations on production requests and disclosure could result from the draft Law on Mechanisms for the Procedural Efficiency of Judicial Public Services, as this draft would extend confidentiality to the negotiating processes regulated by that law as an alternative to judicial proceedings (Article 6).

3 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law. Except in relation to certain legal entities, this Directive will have to be transposed by 17 December 2021.

4 Recommendation adopted by the European Commission on 5 February 2019 for a Council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States on cross-border access to electronic evidence for judicial cooperation in criminal matters.

5 Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings (COM/2018/226 final – 2018/0107 (COD)) and Proposal for a Regulation of the European Parliament and of the Council on European production and preservation orders for electronic evidence in criminal matters (COM/2018/225 final – 2018/0108 (COD)). Both legislative procedures are currently ongoing in the European institutions.

Finally, a new Criminal Procedural Law is being developed. This potential new regulation may have an impact on investigative mechanisms relating to the preservation, request and disclosure of documents; however, it is still too early to assess its impact.

III CONTROL AND PRESERVATION

Spanish legislation does not have a rule setting out a general obligation to preserve data prior to anticipated judicial proceedings (through a litigation hold notice).

The most similar requirement in this respect is that established by Article 30.1 of the Commercial Code, which creates a general obligation for entrepreneurs to preserve accounting files, correspondence, documentation and supporting documents (such as invoices) related to their business activity for six years, which begins from the last day of the company's fiscal year. It has, however, been interpreted that the aim of this obligation is to provide hard copies of the information registered in a company's accounts, and that, consequently, this preservation obligation does not apply to all documentation or correspondence within the company. The ambiguity of the term entrepreneur has led to the interpretation that this obligation is imposed on legal entities as a whole and not on specific natural persons within them.

With the exception of Article 30.1, the regulations on the control and preservation of data are numerous and dispersed. They are only applicable to certain natural and legal persons on the grounds of their professional activities, and only affect certain documents and information. Among the most relevant is Article 25 of Law 10/2010, which establishes an obligation to preserve all data that corroborates compliance with the Law's anti-money laundering obligations. This preservation responsibility extends to:

a all documents related to compliance with know your client obligations;

b data supporting the actual circumstances of transactions carried out with a client; and

c all documents supporting the actual implementation of internal controls with regard to a client and communications made to the anti-money laundering authorities regarding a client or transactions with that client (e.g., any report submitted to those authorities in relation to suspicious transactions).

The obligation to preserve this documentation is imposed on legal and natural persons subject to anti-money laundering obligations listed in Article 2 of Law 10/2010 (including credit institutions and investment firms). This list was broadened by Decree-Law 11/2018, of 31 August to include online gambling providers and to amend the wording of Article 2.1.o).[6] However, case law has not yet reflected the practical consequences of this amendment.

Documents referred to under this Law must be preserved for 10 years from the end of the business relationship with a client, and it is compulsory to destroy these documents after that time period (Article 25).

6 Article 2.1.o was amended to introduce an 'on behalf' clause, its current wording referring to natural persons who, on behalf of a third party, found a company, act as directors or secretaries to the board of directors of a legal entity or act as external advisers, provide a registered office or a trust, or act as shareholders in a company that is not listed on a regulated EU market.

Stock market regulations (primarily the Market Abuse Regulation[7] and the Spanish Stock Market Law[8]) create additional obligations involving the preservation of all documents related to market soundings[9] (including any correspondence and recording of those communications) and insider lists[10] for five years.

The banking and financial field is also subject to numerous preservation obligations. The Stock Market Law requires entities that participate in the securities and investment market to perform and store suitability tests to corroborate the fitness of a specific client to invest in a particular product (which must be safeguarded for five years), as well as samples of the entity's advertising campaigns (although it does not set forth a specific period to conserve this data), among other documentation. There are also supplementary obligations imposed on credit institutions by regulatory entities (e.g., the Bank of Spain) that refer to, for example, the contractual documentation of transactions entered into by those entities (Circular 5/2012 of 27 June).

As a final example, telecommunication companies are also obliged to preserve all data relating to electronic communications or the use of public telecommunication networks for 12 months (Article 5 of Law 25/2007 of 18 October).

From a privacy standpoint, in any of the above-mentioned situations (or in a similar case of preservation of data), in respect of records containing personal data as defined by the EU General Data Protection Regulation (GDPR),[11] this personal data must be erased when no longer necessary for the legitimate purposes for which it was obtained or processed, and which the data subject was informed of and provided consent for (when required). Erasure must lead to the data being blocked (i.e., maintained solely at the disposal of the authorities for the purpose of determining any potential liability arising from its processing, and only for the time during which the liability may arise). When the liability expires, the data must be deleted. Thus, the period during which personal data can be stored must be determined on a case-by-case basis, taking into account the type of personal data and the purposes for which that data is being processed, as well as any possible Spanish legal and statutory requirements.

The sole mention of the preservation of ESI can be found in Article 588 *octies* of the Criminal Procedural Law. This Article allows a public prosecutor and the judicial police to

7 Regulation (EU) No. 596/2014.

8 Law 4/2015 of 23 October.

9 Defined by Article 11.1 of the Market Abuse Regulation as 'the communication of information, prior to the announcement of a transaction, in order to gauge the interest of potential investors in a possible transaction and the conditions relating to it such as its potential size or pricing, to one or more potential investors'.

10 Defined by Article 18.1(a) of the Market Abuse Regulation as 'list of all persons who have access to inside information and who are working for them under a contract of employment, or otherwise performing tasks through which they have access to inside information, such as advisers, accountants or credit rating agencies'.

11 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016. Article 4.1 of the GDPR states that personal data is 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

order any legal or natural person to preserve and protect data or specific information stored in an IT system until the necessary judicial order to permit the seizure and inspection of that data is issued.

IV REQUESTS AND SCOPE

One party (i.e., a legal or natural person) cannot force another party to disclose documents in a pretrial situation (or in a trial) without the intervention of a court. The obligation to provide data in judicial proceedings only arises from a judicial request and in the context of a court case.

Furthermore, as opposed to discovery procedures, a judicial request cannot consist of a general demand for information: Spanish regulations and case law limit the scope of judicial orders to avoid massive requests for data in court proceedings.

This approach is reflected in Article 328.1 of the Civil Procedural Law, which refers to the right of a party to judicial proceedings to request that a counterparty disclose documents. Despite establishing a highly generic obligation to provide information in judicial proceedings (as per the request of a counterparty), Article 328.1 nevertheless limits the scope of the party's request to documents that are not available to the requesting party, and that are related to the subject matter of the proceedings or to the efficacy of the evidence (this limitation on data requests is applicable to all judicial proceedings that fall under the Spanish jurisdiction).

In addition, according to Article 328.2 of the Civil Procedural Law, the requesting party must provide the court with a copy of the requested document or, if this does not exist, a description of its content with as much detail as possible.

A similar approach can be found in a specific regulation that was introduced in 2017 in relation to the civil process to claim for damages for infringements of EU or national competition law (Article 283 *bis* (a) to (k) of the Civil Procedural Law).[12] The amended regulation aims to broaden access to evidence within those cases by setting out a process to request the disclosure of data. However, this new process still requires the intervention of a court to issue a judicial order to gather the relevant documents and information.

The new regulation on these specific proceedings does not permit a general request for information similar to discovery. A party's request must meet different requirements, which may limit the scope of the data demanded. In this regard, at the moment of issuing a judicial order, the court must verify the proportionality of the request, taking into account the following criteria:

a the extent to which the claim or defence is supported by available facts and evidence justifying the request to disclose evidence;

b the scope and cost of disclosure, especially for any third parties concerned, including preventing non-specific searches for information that are unlikely to be of relevance for the parties in the procedure; and

c whether the evidence, the disclosure of which is sought, contains confidential information, especially concerning any third parties, and what arrangements are in place for protecting this information.

12 This regulation amended the Civil Procedural Law pursuant to, among other things, Directive 2014/104/EU of the European Parliament and of the Council of 26 November 2014 on certain rules governing actions for damages under national law for infringements of the competition law provisions of the Member States and of the European Union.

In respect of point (c), the requesting party bears the costs of obtaining the evidence, which are quantified on a case-by-case basis. For this purpose, a court can order a party to provide a guarantee.

In criminal proceedings, further limitations apply, as an investigated party (whether a legal or natural person) cannot be instructed to disclose data because of its right against self-incrimination. Judicial requests can, therefore, only be addressed to third parties (or, at most, to parties to the proceedings that might be held civilly, but not criminally, liable for the alleged offence[13]). To obtain data from an investigated natural or legal person, the court must order a dawn raid and issue an order for the seizure of documents;[14] this approach is also subject to limits set forth by the Criminal Procedural Law (Articles 545 to 578), with the most notable limitations being a prohibition on carrying out futile inspections or seizing documents that are not deemed necessary for the investigation of an offence.

Additional limits set out in the Criminal Procedural Law require that investigative actions be agreed by the court in a judicial writ that is well grounded. Based on the above-mentioned Articles, a judicial order must identify the specific premises where the raid will be carried out, the authority that will be in charge of the inspection and whether the raid will be performed only during the day or also at night. The court's order must be notified to the affected individual, who has a right to be present (or represented) during the inspection. All documents seized during the raid must be numbered by the judicial secretary, and minutes must be drafted, describing how the raid was carried out and listing the documentation that was seized.

In addition to these traditional judicial ways of obtaining data, the Criminal Procedural Law was amended in 2015 to include a detailed regulation on technological investigative measures.[15] Within the amended legislation, Article 588 *sexies* (a) to (c) addresses the inspection of ESI. According to those provisions, the seizure of computers, devices for telephone or electronic communication, or devices for mass storage of information, as well as access to electronic data repositories, must be properly justified by the corresponding court in a judicial order setting out the reasons for agreeing to a request to access that data. The court's order must also set out the scope of the seizure and the necessary measures to be implemented for the preservation of the data.

According to the above Articles, the scope of seizure can be broadened during the course of an inspection to access other devices on which relevant data might be stored, insofar as this possibility has been previously authorised by the court, or otherwise, and in the event of

13 As opposed to other jurisdictions, in Spain, payment for damages resulting from a criminal offence (i.e., civil liability) can be decided within criminal proceedings, together with the criminal liability deriving from the offence. It is the plaintiff's right to choose whether to proceed with the criminal case and civil action at the same time (in a single criminal trial) or not (thus, initiating first the criminal proceedings and, once those are terminated, the civil action before a civil court). The role of strictly civil respondents in criminal proceedings was historically held by legal entities, as criminal liability of corporations was not recognised in Spain until 23 December 2010. Up to that date, in criminal proceedings, legal entities could only be held civilly liable for offences perpetrated by their directors or employees; they could not be subject to criminal conviction.

14 According to Spanish law, a court can also order in the same writ a request for documents and a dawn raid and seizure of these documents to be carried out in the event that this data was not provided voluntarily at the court's request.

15 The amendment was carried out by Basic Law 13/2015 of 5 October, and has been in force since 6 December 2015.

urgency, provided that the judicial authority is immediately informed during the subsequent 24 hours. The court must then confirm or revoke the inspection in the 72 hours following that communication.

Article 588 *sexies* (c)(4) authorises the judicial police, in urgent cases, to directly examine seized devices, provided that this inspection is essential and that they communicate the circumstances to the judicial authorities in the subsequent 24 hours, setting out the reasons for the inspection, its scope, how it was carried out and the results. The court must then confirm or revoke the inspection in the 72 hours following that communication.

The enforcement of the preservation and disclosure obligations described above is enhanced by civil and criminal regulations. Civil regulations establish that failure to preserve or disclose documents requested in litigation must be taken into account by the court when assessing evidence. To that extent, Article 329 of the Civil Procedural Law establishes that a party's refusal to produce any documents requested within judicial proceedings will entitle the court to accept the requesting party's interpretation of the content of those documents as accurate.

In respect of criminal enforcement measures, the Criminal Code prescribes sanctions for specific unlawful acts that are contrary to the preservation and disclosure of data within judicial proceedings. Among those provisions, it sanctions procedural fraud, which is the manipulation of evidence to be used in a party's interest, or any other commission of fraud within the context of judicial proceedings leading to confusion in court that results in a judicial decision that is contrary to the economic interests of the other party to the proceedings or any third party (Article 250(1)(7) of the Criminal Code). Natural persons convicted of this criminal offence will be sanctioned with imprisonment for one to six years and with a fine ranging from €360 to €144,000. For legal persons, the sanction is a fine determined with regard to the economic amount subject to this fraud (which will be multiplied three to five times, depending on the circumstances of the specific offence).

Spanish case law has clarified that 'mere concealment of information' is not criminal, even when the concealed information is 'relevant', as this omission cannot be equal to actually deliberately misleading the court.[16] Therefore, this criminal offence, as interpreted by the courts, does not result in a general obligation to preserve and disclose data.

It is a criminal act to conceal, alter or disable the corpus delicti, the outcome of an offence or the instruments used to commit it with the purpose of impeding the discovery of a criminal offence (Article 451(2)). According to Spanish case law, these concealing actions are sanctioned when carried out:

a knowing (and not only suspecting or assuming) the existence of an offence that is sought to be concealed;

b by someone who has not been involved in the commission of the concealed offence; and

c provided that the action of concealing is performed after the perpetration of the concealed offence.[17]

The length of imprisonment imposed in those cases ranges from six months to three years.

16 Ruling 258/2018, of 29 May, of the Criminal Section of the Supreme Court; Ruling 305/2018, of 20 June, of the Criminal Section of the Supreme Court.

17 Ruling 419/2019, of 24 September, of the Criminal Section of the Supreme Court.

The Criminal Code also punishes disobedience towards the authorities (Article 556), provided that:

a an order that is challenged is final, direct and explicit, and imposes on an individual an obligation to perform (or refrain from performing) a specific action;
b the compelled individual actually knows the content of the order;
c the individual voluntarily disregards the order; and
d the act of disobedience is particularly serious.

However, case law does not require the authority to give prior warning to an individual about the potential criminal consequences of his or her actions, although it is common practice to give notice to that individual. For disobeying the authorities, the Criminal Code establishes a penalty of imprisonment for three months to one year or, alternatively, a fine ranging from €360 to €216,000.

Failure to comply with a judicial order to disclose specific data could, theoretically, be sanctioned as an act of disobedience (assuming that the aforementioned legal requirements are met in a specific case). Court orders reiterating a prior judicial order (e.g., a request to disclose specific documentation) frequently warn corresponding parties of their potential criminal liability for the commission of an act of disobedience if they fail to comply with the order.

This criminal offence is rare in practice. Nevertheless, there are some precedents in case law that should be taken into consideration as they specifically refer to disobedience in connection with a court's order for documentation. For instance, the Criminal Section of the Supreme Court confirmed the conviction of a company's director and shareholder for an act of disobedience involving the failure to disclose a company's accounting files.[18] In its ruling, the Court concluded that the refusal to disclose information or provide documentation ordered by a judge in civil proceedings does not exclude the application of Article 556 of the Criminal Code, regardless of the additional civil consequences that might result from this unlawful behaviour.

These criminal sanctions are in addition to the potential liabilities regarding administrative authorities for the infringement of the applicable obligations to preserve or disclose specific data established in the sectoral regulation referred to in this section.

Privacy regulations should also be taken into account before disclosing documents that may contain personal data, particularly the minimisation and proportionality principles, which require that this data should only be disclosed when it is deemed necessary – with special consideration if sensitive data is involved (e.g., health-related information) – and to assess whether the information can be disclosed anonymously.

V REVIEW AND PRODUCTION

Broad requests for information are rare in Spanish proceedings; thus, the use of advanced technologies for gathering, controlling and reviewing data has not been as necessary in practice as it is in other countries. However, there have been several examples of this type of request in recent years.

18 Ruling 136/2010, of 18 February, of the Criminal Section of the Supreme Court, followed by Ruling 784/2018, of 20 November, of the Court of Appeal of Madrid.

Courts have started to prepare more extensive information requests, especially in the context of competition proceedings and in corporate criminal litigation, where companies are commonly expected to provide much more information than natural persons. In addition to this evolving approach, internal investigations – alien to the legal system until only very recently (and still unregulated) – are gaining importance in the field of criminal enforcement, leading to extensive data review activities, which are characteristic of these investigations.

New technology has also played an important role in this change. Electronic storage of information implies that massive amounts of data are now seized during dawn raids and added to criminal files for analysis by courts and parties to proceedings. In response, the practice of digital forensics, which makes it possible to process enormous amounts of data, has slowly developed in Spain over the past decade and is being used more frequently.

Experience shows that when dealing with those kinds of situations, lawyers tend to involve a forensics company to ensure the proper preservation and review of data. However, law firms are still in charge of directing investigations and making strategic decisions, and the intervention of an attorney remains necessary for an investigation to be subject to legal privilege. Forensics companies have implemented some of the international techniques for the analysis of information (e.g., software tools to carry out keyword searches and corporate intelligence resources). However, use of predictive coding and email threads is not yet widespread, with the exception of their use in cross-border internal investigations, where more sophisticated IT tools usually apply.

The experience has been similar with regard to legal privilege. The limited content of judicial requests for information (together with the fact that internal investigations have not played an important role in Spain thus far) has traditionally implied that legal privilege is not as frequently challenged in Spain as it is in other countries. Therefore, discussions about the exact scope of this privilege have not been common, so its limits are not as defined as in other jurisdictions. However, this is likely to change now that the scope of judicial demands has expanded, and internal investigations are increasing in importance. The new Lawyers' General Statute[19] that will enter into force on 1 July 2021 already includes some developments in this area.

Notwithstanding additional potential future changes, the definition of privilege is particularly broad. According to the Basic Law on the Judiciary (Article 542.3), privilege protects all facts or information known by lawyers as a result of any form of their professional activity. Article 22.1 of the new Lawyers' General Statute details the scope of privilege and establishes that it relates to any facts, communications, data, information, documents and proposals known, issued or received by lawyers as a result of their professional activity.

The Lawyers' Deontological Code, approved on 6 March 2019 by the General Council of the Spanish Bar, attempts to define the concept's scope more precisely. According to the Code, facts or information known by lawyers as a result of any of the forms of their professional activity include:

a any confidential information or proposal received by a lawyer from his or her client, a counterparty and other colleagues;

b any documents sent or received by a lawyer as a result of any of the forms of his or her professional activities; and

19 Although the law, passed by the Council of Ministers on 2 March 2021, has not been published yet, the draft regulation is publicly available and no changes to this latest draft were announced.

c any communications exchanged between lawyers, including negotiations, whether oral or written.

The Deontological Code is not positive law, but rather a professional code of conduct that binds lawyers to a set of ethical standards that courts may or may not apply in their interpretation of the law.

The law does not expressly refer to the work-product doctrine (i.e., notes prepared by the lawyer for internal purposes only), although it is generally accepted that the protection of legal privilege also extends to documents that involve the relaying of facts by a client and legal advice on those matters.

With regard to the exceptions to legal privilege, some comments must be made regarding in-house lawyers and anti-money laundering regulations.

The extension of legal privilege to in-house lawyers has traditionally been a matter of debate as Spanish legislation and European rulings are not entirely aligned. According to the Court of Justice,[20] in-house lawyers and external lawyers are in distinct situations, given the hierarchical integration of the former within the company that employs them. As a result, the principle of equal treatment is not infringed by the fact that legal professional privilege is not acknowledged in relation to in-house attorneys.

However, the Spanish regulations would not establish a similar distinction between the two types of lawyers. In addition, there would be no consolidated Spanish case law in this regard, thus the confusion governing this field.

The new Lawyers' General Statute seems to accentuate the different positions of the Court of Justice and the Spanish legislation as this new regulation expressly includes legal privilege among the principles applicable to in-house lawyers. In practice, the European approach to this matter would be taken into consideration by Spanish lawyers. This more cautious approach might change in the coming years owing to the new Spanish regulation, although it will depend on how the Spanish courts interpret this new legal provision.

In respect of exceptions to legal privilege foreseen by anti-money laundering regulations, as from the Second Anti-Money Laundering Directive (Directive 2001/97/EC), the European Union has established that lawyers must report any suspicions of money laundering unless they are ascertaining the legal position of a client or representing a client in legal proceedings (or in relation to legal proceedings, including legal advice on the initiation or avoidance of legal proceedings – see Article 22 of the Anti-Money Laundering Law). This scope of privilege is significantly more limited than the general definition in the Basic Law on the Judiciary and the Lawyers' General Statute.

Finally, the initial draft for the incorporation into Spanish law of Council Directive (EU) 2018/822 of 25 May[21] (published on 20 June 2019) does not limit the legal professional privilege of tax advisers, contrary to what was initially expected in the legal sector.

20 Ruling in Case C-550/07 *P, Akcros Chemicals Ltd v. the European Commission*.

21 Directive on mandatory automatic exchanges of information in the field of taxation in relation to reportable cross-border arrangements.

VI PRIVACY ISSUES

The legal framework for the protection of personal data in Spain is regulated by the Lisbon Treaty, Article 18(4) of the Spanish Constitution, the GDPR and the Spanish Basic Law 3/2018 of 5 December on data protection and digital rights guarantees.

Neither the GDPR nor Basic Law 3/2018 contain specific provisions regarding e-discovery and information governance. Sector-specific regulations also do not contain any data protection provisions on those matters.

For the discovery process to take place lawfully, the processing of personal data must be legitimate and satisfy one of the grounds set out in Article 6 of the GDPR (if the information is sensitive personal data, it also needs to satisfy one of the conditions in Article 9 of the GDPR). If personal data is intended to be obtained by screening the corporate emails of the relevant employees or from other devices located in the workplace, such as the video recording systems, Articles 87 and 89 of Basic Law 3/2018 must also be observed.

Article 6.1(c) of the GDPR establishes that processing must be lawful if it is necessary for compliance with a legal obligation to which a controller is subject. However, non-EU laws are not considered, as such, a legal basis per se for data processing, in particular regarding transfers to foreign authorities and especially if they are public authorities. In this regard, the Spanish Data Protection Authority understood in its Report 2011-0469 that US civil procedure law cannot be included within the concept of law that legitimates data processing.

This approach is consistent with Article 6.3 of the GDPR, which states that the basis for the processing referred to in point (c) of Article 6.3 must be laid down in EU law or in the law of the Member State to which the controller is subject. Therefore, e-discovery and any enforcement requests based on those laws require a complex case-by-case analysis from a data protection standpoint.

Personal data transfers to countries that do not ensure an equivalent level of protection are permitted only if a controller or processor has provided appropriate safeguards,[22] and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available, unless a legal exception to Article 49 of the GDPR applies.

These derogations have been analysed in Guidelines 2/2018 on Article 49 of Regulation 2016/679, adopted by the European Data Protection Board. According to this joint position, Article 49(1)(e) (which states that a transfer could be deemed legitimate to the extent that it is necessary for the establishment, exercise or defence of legal claims) may cover a range of activities, for example, in the context of a criminal or administrative investigation in a third country (e.g., antitrust law, corruption, insider trading or similar situations), where the derogation may apply to a transfer of data for the purpose of an individual defending himself or herself, or for obtaining a reduction or waiver of a fine that is legally foreseen (e.g., in antitrust investigations).

Data transfers for the purpose of formal pretrial discovery procedures in civil litigation may also fall under this derogation. It can also cover actions by a data exporter to institute procedures in a third country (e.g., commencing litigation, seeking approval for a merger). Notwithstanding this, a derogation cannot be used to justify the transfer of personal data on the grounds of a mere possibility that legal proceedings or formal procedures may be brought in the future.

22 The European Data Protection Board adopted Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data in November 2020.

According to the data minimisation principle, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is disclosed. For that reason, the Spanish Data Protection Authority encourages – when feasible – the anonymisation of information (or pseudonymisation, as the case may be). It has issued some guidelines in this regard, including the 'Guidelines and guarantees in the process of personal data anonymisation' dated July 2018 and 'Introduction to hash as a pseudonymisation technique for personal data' dated October 2019.

Finally, the disclosure of personal data requires providing prior notice of the possibility of personal data being transferred to and processed by foreign authorities. If recipients are established in non-equivalent countries, specific information on the existence of an international transfer must also be provided.

VII OUTLOOK AND CONCLUSIONS

Given the absence of an overarching process for the regulation of discovery, the preservation and disclosure obligations applicable in a specific case vary significantly depending on the context in which the obligations are raised. Thus, determining the applicable obligations requires a case-by-case assessment that must take into consideration factors such as the business activity of the corresponding legal or natural person from whom the information is being sought.

In general, the consequences of failing to comply with these preservation and disclosure obligations also vary significantly depending on the circumstances of an infringement.

In addition to a lack of uniformity, discovery is a developing field in Spain that has evolved rapidly in recent years. A new legal framework and practice (especially regarding digital forensics) can be expected in the coming years, and some steps are already being taken towards establishing this uniform framework (particularly triggered by new European regulations on e-discovery-related matters).

Appendix 1

ABOUT THE AUTHORS

ENRIQUE RODRÍGUEZ CELADA

Uría Menéndez Abogados, SLP

Enrique Rodríguez Celada is counsel in the Madrid office of Uría Menéndez. He joined the firm in 2008.

Enrique's practice focuses on white-collar crime. He has taken part in complex criminal proceedings involving fraudulent bankruptcy, tax crime, fraud, corporate crime, corruption, subsidy fraud and crimes against workers' rights, among other things. Enrique also has experience in litigation with international implications (e.g., letters rogatory or the enforcement of foreign judgments) and in the coordination of clients' legal defences in various jurisdictions.

He also advises clients on matters regarding the criminal liability of corporations, which includes preparing and reviewing compliance programmes, implementing anti-corruption policies and leading internal investigations.

Enrique is an associate lecturer on the law degree programme of IE University (Madrid), where he lectures on criminal procedural law. He also lectures on issues regarding the criminal liability of corporations and internal investigations on a master's degree programme at the International University of La Rioja.

SARA SANZ CASTILLO

Uría Menéndez Abogados, SLP

Sara Sanz Castillo is a lawyer in the Madrid office of Uría Menéndez. She joined the firm in 2013.

Sara advises companies, as well as their directors and employees, on corporate criminal law. She has experience in criminal proceedings dealing with a wide range of criminal offences (tax fraud, corporate criminal offences, offences against the environment and offences against workers' rights, among other things). She also has experience in advising companies on the development and implementation of compliance programmes, as well as on conducting internal investigations.

Sara is an associate lecturer on the law and business administration programme of CEU San Pablo University (Madrid), where she lectures on criminal procedure law.

REYES BERMEJO BOSCH

Uría Menéndez Abogados, SLP

Reyes Bermejo Bosch is a lawyer in both the Madrid and Valencia offices of Uría Menéndez. She became a lawyer in 2006 and joined the firm in 2011.

She focuses her practice on data protection, e-commerce and IT. Reyes provides national and multinational companies with day-to-day advice in the above-mentioned areas on matters such as privacy, consumer protection and e-commerce, and dealings with public authorities, including the drafting and negotiation of IT agreements. In particular, she has extensive experience in the data protection design of commercial and M&A transactions; the preparation of notices, clauses, contracts, protocols and training programmes; authorisation proceedings for international transfers and administrative and judicial proceedings; the preparation of website terms and conditions and cookie policies; and advising on direct marketing activities by electronic means.

Reyes is also a professor of data protection and e-commerce law on various master's degree programmes and seminars.

She contributes to the firm's data protection newsletter and legal magazine, *Actualidad Jurídica Uría Menéndez*, on aspects of, and updates relating to, data protection regulatory issues and case law.

URÍA MENÉNDEZ ABOGADOS, SLP

C/Príncipe de Vergara, 187
Plaza de Rodrigo Uría
28002 Madrid
Spain
Tel: +34 915 860 400
enrique.rodriguez@uria.com
sara.sanz@uria.com
reyes.bermejo@uria.com
www.uria.com

an LBR business

ISBN 978-1-83862-772-0