THE e-Discovery and Information Governance Law Review

Editor
Tess Blair

THE LawReviews

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW

Reproduced with permission from Law Business Research Ltd
This article was first published in July 2019
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Tess Blair

THE LAWREVIEWS

PUBLISHER
Tom Barnes

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Joel Woods

SENIOR ACCOUNT MANAGERS
Pere Aspinall, Jack Bagnall

ACCOUNT MANAGERS
Olivia Budd, Katie Hodgetts, Reece Whelan

PRODUCT MARKETING EXECUTIVE
Rebecca Mogridge

RESEARCH LEAD
Kieran Hansen

EDITORIAL COORDINATOR
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Tessa Brummitt

SUBEDITOR
Caroline Fewkes

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-912228-76-8

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

© 2019 Law Business Research Ltd

ACKNOWLEDGEMENTS

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

ALLENS

BLAKE, CASSELS & GRAYDON LLP

BOMCHIL

FÉRAL-SCHUHL / SAINTE-MARIE

KLA – KOURY LOPES ADVOGADOS

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA 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 first 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. Although e-discovery is common in some countries, such as the United States, it remains a foreign concept – sometimes unheard of – 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.

Information governance is likewise an intricate issue, involving the organisation, maintenance, use and disposition of information in light of business goals, and 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.

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 first edition of *The e-Discovery and Information Governance Law Review*. We would also like to thank the Law Reviews, without which this work would not have been possible.

Tess Blair
Morgan, Lewis & Bockius LLP
Philadelphia
May 2019

Chapter 1

ARGENTINA

Adrián Furman, Martín Torres Girotti and Catalina Malara[1]

I OVERVIEW

Discovery is defined as 'compulsory disclosure, at a party's request, of information that relates to the litigation'.[2] This pretrial stage consists of requests for admission of certain facts, performance of interrogatories, requests for production of documents and depositions, among others. The aim of this procedure is to avoid 'surprise evidence' at trial, but it can also encourage settlement.

In Argentina, this process is neither available nor regulated. The process for the offering and collection of evidence, including electronically stored information (ESI), is a matter subject to judicial control. Upon filing and responding to a judicial complaint, each of the parties has the right to offer and produce, within the judicial file and under the court's direction and control, the evidence it deems necessary and appropriate to prove its statement and justify its arguments. In this scenario, a party may resort to broad means of proof, including documents or information held by the counterparty or even by third parties.

The above, however, does not preclude the rights of a party to collect or produce the necessary evidence (including ESI) prior to the formal commencement of a litigation or the allocated time for evidence to be produced in a litigation. Regulations regarding different forms of obtaining pretrial evidence are contained in each province's procedural code.[3] Although every province has its own particularities, most procedural codes recognise three ways in which a plaintiff (or a defendant, when applicable) may require the production of evidence prior to a litigation: preliminary investigations, anticipated proof and interim measures. The decision in each instance must be authorised by the court.

Preliminary investigations are available for those who intend to sue or who, with reasonable grounds, expect to be sued.[4] They provide the opportunity to obtain certain information needed for the claim or the response, without which the process could not take place. Although this measure is requested prior to the trial (which is the same for discovery), it is always requested before a court of law. If it is possible to obtain the information through extrajudicial means, the request for preliminary investigations shall not proceed.

Even though each procedural code mentions different situations in which preliminary investigations can be requested, case law has recognised that those are only examples, and that any similar measure requested to comply with the aim of the procedure may be granted

1 Adrián Furman and Martín Torres Girotti are partners, and Catalina Malara is an associate, at Bomchil.

2 *Black's Law Dictionary* (Seventh Edition), p. 478.

3 Under Argentine law, each province has its own procedural code. However, the Civil and Commercial Code applies to all provinces.

4 Article 323, National Procedural Code.

by the judge if it is needed for the claim or response, as applicable. The plaintiff in a case concerning inheritance, for example, may request that a will be exhibited if he or she believes that he or she is an heir and there is no way of obtaining the will without going to the courts. This amounts to a preliminary investigation.

Anticipated proof may be requested by a party that is or will be part of a claim and has justified reasons to believe that it will be impossible or very difficult to produce evidence during the litigation.[5] The National Procedural Code (Article 326(2)) provides that anticipated proof can be requested to obtain 'judicial recognition or an expert opinion to record the existence of documents, or the status, quality or condition of things or places'. Additionally, subsection 4 states that 'the exhibition, safekeeping or seizure of documents concerning the object of the claim' can also be requested. In both cases, ESI can be requested through the use of this procedure. Anticipated proof means that the plaintiff can obtain evidence outside the usual time frame (that is, after filing or responding to a claim), which can then be preserved. It is a measure that is permitted in exceptional circumstances and only when deemed essential. The request for anticipated proof is also usually granted without the prior involvement or participation of the counterparty.

Finally, interim measures may be requested before or after a claim is filed, and aim to protect a party's assets, rights or proof when it is not possible to wait for the final resolution of the claim to obtain them (e.g., in a case concerning construction, a party may request the court to suspend the work being done if, by the time the resolution is final, the damage will be irreparable).[6] They are usually granted without the prior involvement and participation of the counterparty.

Regarding payment of costs, although there are some exceptions, the losing party shall pay all costs and fees related to the claim,[7] including all measures requested by the winning party.

II YEAR IN REVIEW

No change in legislation regarding ESI is expected to happen in the near future. Nevertheless, each year additional case law dealing with different forms of ESI is established and, in particular, with different ways of ensuring its access and preservation. Courts have been setting a trend that allows a more flexible interpretation regarding ESI, which equates the effects of ESI with those of written documents.

A few years ago, courts were more reluctant to give full evidential value to different forms of ESI (e.g., emails or text messages). In a case in 2007, the National Commercial Court of Appeals[8] stated that an email that did not comply with the requirements set forth in the Digital Signature Law[9] could not be given evidential value, because the authentication provided by the digital signature was essential.

5 Article 326, National Procedural Code.

6 Articles 195 et seq., National Procedural Code.

7 Article 68, National Procedural Code.

8 National Commercial Court of Appeals, Chamber D, 16 February 2007, *Henry Hirschen y Cía SA v. Easy Argentina SRL*.

9 Law 25,506.

In recent years, courts have been more flexible with their interpretation of ESI as a means of proof.[10] In a case in 2014, the court decided that 'if the email has been sent without an electronic signature, the court must weigh it according to the rules of rational criticism, taking into account whether it has been recognised or not by the party against whom it is intended to assert; if an informatics analysis has been carried out in that case to demonstrate its authenticity and inalterability determining the date of sending, sender, recipient, attachments, etc.'.[11] Therefore, the incorporation of a digital signature has become less important when determining the evidential value of an email (or any other ESI) – it has been recognised that the key factors to consider are authenticity and lack of alteration. Experts that are able to assess whether ESI has been tampered with or if it is authentic have been allocated more important roles by the courts.

Case law has also been establishing the requirements for ESI to be disclosed before trial through one of the three methods of pretrial production of evidence mentioned in Section I. The argument that the opposing party is in a position to hide or destroy certain documents is not sufficient for a court to grant and allow the production of anticipated proof. It is necessary to demonstrate, at least summarily, that the party intends, or has indicated its intention, to do so, especially if the party requesting disclosure seeks a surprise seizure of documents or ESI.[12]

III CONTROL AND PRESERVATION

There are no specific rules regarding control in the context of ESI, therefore general procedural rules apply. These rules state that a court must order a party in possession of evidence to produce it within a specific time.[13] If the party does not produce the evidence and does not provide a sound reason and, based on other elements of judgement, the existence of the evidence and its content are manifestly credible, there will be a presumption of guilt. The concealment of evidence can be considered proof that the evidence exists. In certain cases, the non-disclosure can be justified, for example, because of attorney–client privilege (see Section V).

Adverse inferences are the only sanctions that the law applies to parties that do not produce – or preserve – evidence under their control, when required to do so. Parties are not subject to a duty (failure of which would be penalised) or an obligation (compliance with which could be coercively demanded by the other party), but they are constrained by a procedural burden of good faith and collaboration in the production of evidence, which governs the entire litigation process and, specifically, the preservation and production of evidence that could be in the parties' control. If this procedural burden is breached, it could mean that the party in question is deemed to have evidence that is harmful to its case.[14]

Case law has stated that procedural law fails to impose on the parties duties and procedural obligations, but places the emphasis on the burden of proof. The burden of proof is a procedural notion that enables the judge to evaluate the evidence to decide a

10 Molina Quiroga, Eduardo, 'Evolución de la jurisprudencia en Derecho Informático', *SJA* 11 July 2018.

11 Civil and Commercial Court of Appeals of Córdoba, First Chamber, 22 May 2014, *Pisanu, Juan Mauro v. Carteluz SRL s/ ordinario Otros*.

12 Scotti, Héctor Jorge, 'Una interesante resolución en materia de prueba anticipada'.

13 Article 387 et seq., National Procedural Code.

14 *Código Procesal Civil y Comercial de la Nación: Comentado y Anotado*, Kielmanovich, Jorge L.

case when there is no certainty about the facts that should be the basis of the decision. It also establishes which of the parties is interested in proving the facts in order to avoid unfavourable consequences.[15]

Preservation of ESI is a complex subject. Although Argentine legislation does not have any specific rule determining the length of time that ESI must be kept, the Civil and Commercial Code[16] stipulates that, in general, documents should be preserved for 10 years. Therefore, it is reasonable to assume that ESI should also be preserved for 10 years. Preservation not only implies not destroying the records, but also maintaining them so that they do not suffer deterioration due to the passage of time or exposure to any harmful elements, allowing them to be consulted or made available if required. With regard to ESI, it will be necessary to guarantee its authenticity, so that the origin of the information is certain.[17]

IV REQUESTS AND SCOPE

Even though the parties to a lawsuit are not obliged to meet in the context of disclosure of ESI that may be useful for a lawsuit (nor are there lists drawn up to obtain the information), there are certain rules that parties should abide by regarding the request for and scope of the production of evidence. These rules would apply to ESI.

The first rule is the duty to offer evidence on time. In every lawsuit, the parties must file the documentary evidence on which their case is based. The law explicitly establishes that the documentation the parties possess must be submitted by them when filing the complaint or upon answering the complaint, as applicable. This duty forbids the parties from submitting documentation at other times, unless it refers to documentation that has come to their attention later in the process. They must stipulate under oath or in a statement that they had no knowledge of it when the claim started.[18] If, according to reasonable criteria, the existence and contents of the documents are credible, failure to present them will result in a presumption that they are harmful to the party's case.[19]

Moreover, when the documentary evidence is not available, the party in question must provide a description of it, including its contents, location and details of the public agency or individual holding it.

The second rule is the duty to present the essential documents for the resolution of the dispute. Article 387 of the Civil and Commercial Code provides that: 'The parties and third parties who have essential documents for the resolution of the dispute shall be obliged to present them or to indicate the notarial record or file where the original documents are kept.'

Regarding documents in the possession of third parties, Article 387 provides (as a general principle that also applies to ESI) that third parties shall be sent a notice of demand to present the documents, and that those parties may (1) present the documents requested at trial or (2) object to their presentation if the documents are exclusively owned by them and

15 National Commercial Court of Appeals, Chamber C, *Bellini, Gabriel y otro v. Lee, José L*, 26 May 1995.

16 Article 328, Civil and Commercial Code.

17 Comments on Article 328, Civil and Commercial Code. Marisa Herrera, Gustavo Caramelo and Sebastián Picasso.

18 *Código Procesal Civil y Comercial de la Nación: Concordado con los códigos provinciales. Análisis doctrinal y jurisprudencial*, Elena I Highton – Beatriz A Areán, Volume 6, p. 381.

19 Article 388, National Procedural Code.

disclosure may cause them harm. In the latter case, the notice of demand may be dismissed and the third party may be released from the duty to present documents if the objection is duly grounded.[20]

The third rule relates to the burden of proof, construed as the legal principle that determines who is obliged to prove a certain fact before the court. The general principle[21] is that the burden of proof shall be borne by the party affirming the existence of a controversial fact or of a legal provision that the court does not have a duty to know (excluding, therefore, the applicable law). Each party must prove the facts on which it is grounding its claim, defence or motion. Because of this duty (as provided by civil procedure), the powers of the court to order evidence, on its own initiative, are exceptional and incidental.

However, when establishing the applicable principles for civil liability, Article 1735 of the Civil and Commercial Code provides that 'the judge may distribute the burden of proof or, having acted with due diligence, may consider which party is in a better position to provide it.'[22] This Article includes the principle of dynamic burden of proof, which means that, exceptionally and taking into account the circumstances of each case, the court may shift the burden of proof to the party that is in a better position to provide evidence, or, if there is little or no evidence, to the party that is in a better position to prove the facts of its case.

V REVIEW AND PRODUCTION

The use of advanced analytical tools is not prevalent in the analysis, review and production of evidence.

Communications between a lawyer and his or her client are protected by attorney–client privilege, which is found in different laws, procedural codes and the Constitution. Attorney–client privilege is very strict and provides lawyers with many tools to avoid being forced to produce evidence in their power delivered to them by their clients, subject to the fact that they were acting as their attorneys.

For example, in a very famous case in Argentina, a lawyer filed a claim to declare the unconstitutionality of a law and its regulatory decree that imposed an obligation for telephone companies to record certain information in telephone communications. His arguments included that this constituted a violation of his rights to privacy, but also that it harmed the privilege of confidentiality that, as a lawyer, he holds in communications with his clients. The Supreme Court ratified the decision taken by the lower courts and stated that this legislation was in fact unconstitutional as it did not respect the right to privacy and professional secrecy.

A lawyer is only permitted to reveal information when (1) the client allows him or her to do so, (2) when the information is necessary for the attorney's own defence and (3) when a competent judge authorises the attorney to reveal it, for reasons that must be expressly indicated and assessed. If the lawyer produces the privileged information and one of the above exceptions does not apply, he or she will be subject to penalties. The court must not, however, take it into account when deciding on the matter.

20 id., footnote 14.

21 Article 377, National Procedural Code.

22 Article 1735.

The work-product doctrine does not exist in Argentina. However, we believe that a lawyer's work-product is protected by attorney–client privilege. If a lawyer is requested to produce his or her work-product in a trial, the same protection granted for communications must apply as the work-product originated from the information provided by the client.

As mentioned in Section III, the court determines the time frame within which parties must produce the evidence. According to the National Procedural Code, the time frame should not exceed 40 working days. In practice, however, it lasts much longer as the courts extend it as long as is necessary to have all the proposed evidence duly produced.

As stated in Section IV, only evidence that is directly related and essential to the case can be offered in trial. If evidence is protected under contractual or legal confidentiality, or if the type of evidence being brought is not admitted by the law or cannot be admitted for procedural reasons, then a party can challenge the production of it. Additionally, a party may argue that the evidence produced is against public policy or morals and request that it be considered 'confidential' and only made available to the involved parties.

If a party fails to comply with these obligations, which would also apply to ESI, then the court may impose progressive pecuniary sanctions aimed at ensuring that the party complies with its mandate. The amount of the sanctions will be determined by the court in favour of the party affected by the breach.

VI PRIVACY ISSUES

The Data Protection Law[23] defines personal data as information of any type that refers to determined or determinable natural or legal persons.[24] If ESI to be disclosed contains personal data, then the Data Protection Law and its regulatory decree[25] are applicable.

Handling of personal data always requires the consent of the data owner. One of the exceptions set forth in the Data Protection Law is when the personal data is collected for the exercise of functions proper to the powers of the state or by virtue of a legal obligation. When the handling of personal data is required under one of the three methods of obtaining pretrial evidence (see Section I), the court will exercise its judicial power to request it. The consent of the data owner is not required in these cases.

Regarding cross-border transfers, the Data Protection Law states that the transfer of personal data (of any kind) with countries or international or supranational organisations that do not provide adequate levels of protection is prohibited. However, if the cross-border transfer is requested as part of an international judicial cooperation process, the prohibition will not apply.

If an Argentine party wishes to produce evidence that has been requested internationally, it must ensure that the evidence complies with Argentine law.

Additionally, the Confidentiality Law[26] states that individuals or legal entities may prevent information that is legitimately under their control from being disclosed to third parties, or acquired or used by third parties in a manner contrary to honest commercial practices, provided that the information (1) is confidential, in the sense that it is not generally known or easily accessible to persons in that field of work, (2) has commercial value

23 Law 25,326.

24 Article 2.

25 Regulatory Decree 1558/2001.

26 Law 24,766.

because it is confidential and (3) the person who controls it has taken reasonable measures to keep it confidential. ESI is specifically considered when the Law details how 'confidential information' can be stored.

VII OUTLOOK AND CONCLUSIONS

Although it is unlikely that any specific law regarding ESI – or disclosure as part of procedural law – will be passed in the coming years, the laws regarding production and preservation of evidence need to be updated to cover all measures that can be used in litigation. Courts have been updating the cases where ESI can be produced in the past years, since they are the ones that are presented with real cases and have the need to protect plaintiffs and defendants requesting their collaboration regarding preservation and production of ESI, mainly when it is under the other party's control.

It is expected that the rules applicable to pretrial production of evidence will continue to be made more flexible, as a lot of information is now stored electronically and a delay in its production can mean that evidence is lost.

Chapter 2

AUSTRALIA

Ross Drinnan, Michael Morris, Samantha Naylor Brown and Phoebe Boyle[1]

I OVERVIEW

Litigation in Australia is conducted in different federal, state and territory courts depending on the nature of the matter at hand and the relevant laws in question. Practice and procedure and, consequently, approaches to electronic discovery (e-discovery) vary between those courts; however, generally, the exchange of electronically stored information (ESI) is commonplace in the discovery process.

The use of technology to assist with review has been prevalent in most Australian jurisdictions for several years and key word searching, email threading and deduplication are accepted practices. The use of more advanced analytical tools, such as predictive coding, is still developing but has been agreed to by parties and courts as an appropriate method to review and produce documents. The approach to ESI has developed through a combination of practice, case law and adjustments to rules and procedure.

In the first instance, the cost of discovery (or disclosure) is generally borne by the party making the discovery; however, in some cases, an order may be made that a party requesting discovery pay for some or all of the estimated costs of discovery in advance, or give security for the payment of the cost of discovery.[2] Depending on the outcome of the litigation, costs may be awarded against a losing party, requiring it to reimburse the party making discovery for some or all of the costs associated with the discovery.

Sources of law and regulation governing discovery

The Federal Court of Australia (the Federal Court) has original jurisdiction to hear both civil and criminal matters relating to Commonwealth law (although certain criminal matters are still heard by state courts) at the federal level.[3] The Federal Court also has an appeals court, the Full Court of the Federal Court of Australia, which has appellate jurisdiction in relation to matters heard in its original jurisdiction.

---

1 Ross Drinnan and Michael Morris are partners, Samantha Naylor Brown is an associate and Phoebe Boyle is a lawyer at Allens.

2 See Federal Court Rules 2011 (Cth) r 20.13; Civil Procedure Act 2010 (Vic) s 55(4).

3 Although, at the time of writing, the federal government is considering expanding the jurisdiction of the Federal Court, such that it has jurisdiction to hear criminal matters under the Corporations Act 2001 (Cth). Jurisdiction for these matters has historically rested with state courts: Australian government, 'Restoring trust in Australia's financial system: The Government response to the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry' (February 2019) 39.

The Federal Court of Australia Act 1976 (Cth), the Federal Court Rules 2011 (Cth) and practice notes issued by the Court are the primary source of requirements relating to practice and procedure in that jurisdiction.[4] In regard to discovery and, in particular, e-discovery, the primary sources of rules are:

a Part 20 of the Federal Court Rules 2011 (Cth);

b Section 10 of the Central Practice Note: National Court Framework and Case Management; and

c the Technology and the Court Practice Note (GPN-TECH).[5]

State and territory courts handle matters relevant to the laws in each of those jurisdictions. In each state and territory, the highest court is the supreme court but the structure of lower level courts vary. For example, in New South Wales, the court structure consists of three tiers: the Local Court, the District Court and the Supreme Court. The supreme court in each state or territory generally has a trial division with original jurisdiction for matters that reach a certain threshold (e.g., reflecting the monetary value of the issue in dispute or the seriousness of the offence), as well as an appeals division with appellate jurisdiction for matters from its own trial division and lower courts.

Like the Federal Court, practice and procedure (including for discovery and e-discovery) in most state and territory supreme courts is governed by a set of rules in combination with practice notes and directions issued by the relevant court. In most cases, the rules applicable to civil matters differ from those applicable to criminal matters. In several states and territories, in the civil jurisdiction, a uniform set of rules has been adopted to streamline practice and procedure.[6]

The High Court of Australia is the highest court in Australia and it has original jurisdiction to hear matters related to the Australian Constitution and appellate jurisdiction to hear matters from the appellate courts at the federal, state and territory level. The High Court Rules 2004 primarily govern procedure in that court.

This chapter focuses on e-discovery and information governance practices in the Federal Court and highlights particular points of difference or interesting approaches in the supreme courts of the states and territories. It does not consider all differences between the various supreme court jurisdictions nor address lower-level courts in states or territories. As practice and procedure differ between courts across Australia, care should be taken to consider the applicable legislation, rules and guidance for the court in which a party is appearing.

II YEAR IN REVIEW

There have not been any significant case law developments in the past 12 months that relate to e-discovery or ESI. The most significant recent case occurred in 2016 and involved the Victorian Supreme Court's approval of predictive coding as part of a party's reasonable searches when giving discovery.[7]

4 There are also specific rules that apply to certain matters, for example, the Federal Court (Corporations) Rules 2000, which contain specific provisions related to corporations matters heard by the court.

5 Federal Court of Australia, Technology and the Court Practice Note, 25 October 2016.

6 See, e.g., the Uniform Civil Procedure Rules 2005 (NSW).

7 *McDonnell Dowell Constructors (Aust) Pty Ltd v. Santam Ltd (No 1)* (2016) 51 VR 421.

While the approach taken by practitioners to ESI is well developed in all jurisdictions, court guidance on how parties should approach e-discovery and ESI is progressively catching up with practice in the legal industry. For example, the Australian Capital Territory (ACT) and Queensland Supreme Courts have recently updated their guidance in this area.

In the ACT, Practice Direction No. 3 of 2018 took effect on 1 January 2019. Paragraphs 14 and 15 of the Direction deal with e-discovery in civil proceedings and suggest that parties should give early consideration to formulating a discovery plan that addresses, among other things, 'the search/review process and the use of procedures to remove repeated or duplicate content' and exchanging documents 'having regard to the importance of preserving original metadata'.

In Queensland, Practice Direction No. 18 of 2018, titled 'Efficient conduct of civil litigation', was published on 17 August 2018. The direction requires parties 'to confer and agree a basic plan for the management of documents'[8] and includes a sample form for such a plan in an appendix. The sample plan suggests that deduplication and the use of key word searches to identify relevant documents should be considered.[9]

III CONTROL AND PRESERVATION

i Control

The Federal Court Rules 2011 (Cth) specifically state that 'document' includes the definition in the Evidence Act 1995 (Cth) 'and any other material, data or information stored or recorded by mechanical or electronic means'.[10] While the same definition is not included in all legislation and rules, it is generally accepted practice that electronically stored documents are caught by the terms 'document' and 'any record of information'. A document must be (or have been) within a party's control to be discoverable.[11]

While the precise wording varies between states, in most jurisdictions this means that a party must disclose a document if it is (or was) in their possession, custody or power.[12] Generally, for the purposes of discovery, 'custody' refers to the actual holding of the document,[13] 'possession' means the physical holding of the document pursuant to a right of its possession (as in the case of an agent or bailee) and 'power' is understood as an enforceable right to obtain possession or control from the person who has custody over it.[14]

8 Supreme Court of Queensland, Practice Direction No 18 of 2018: Efficient Conduct of Civil Litigation, 17 August 2018.

9 Supreme Court of Queensland, Appendix to Practice Direction No 18 of 2018: Efficient Conduct of Civil Litigation, 17 August 2018, paras 5, 8, 11.

10 Federal Court Rules 2011 (Cth) Dictionary sch 1 (definition of 'evidence').

11 See, e.g., Federal Court Rules 2011 (Cth) r 20.14(1)(c); Uniform Civil Procedure Rules 1999 (Qld) r 211(1)(a).

12 See Civil Procedure Act 2005 (NSW) s 3 (definition of 'possession'); Uniform Civil Procedure Rules 2005 (NSW) r 21.3(2). Note that in Queensland, a party must disclose a document if it is in their possession or under their control (r 211(1)(a)).

13 See *Roux v. Australian Broadcasting Commission* [1992] 2 VR 577; *Commissioner of Taxation (Cth) v. Australia and New Zealand Banking Group Ltd* (1979) 143 CLR 499.

14 Although note that in some jurisdictions, the right may not need to be recognised in law or equity, see Supreme Court Civil Rules 2006 (SA) r 4; *Reid v. Langlois* (1849) 41 ER 1408; *B v. B* [1978] 3 WLR 624; *Lonrho Ltd v. Shell Petroleum Co Ltd* [1980] 1 WLR 627; *Psalidis v. Norwich Union Life Australia Ltd*

In the context of ESI, this raises unique issues, for example, where a document is stored on the server or database of a third-party provider, a party may not physically hold the information that is sought. However, as noted above, the obligation to provide discovery extends to documents over which a party has power or custody, and if a party has a legal right to obtain the ESI from its third-party provider, it will have the requisite control for the purposes of discovery.

ii Preservation

There is a myriad of obligations to retain information and documents under federal and state legislation. These obligations are sourced from a range of statutes and apply to information irrespective of its possible or likely use in a litigious or regulatory matter. For example, Section 286 of the Corporations Act 2001 (Cth) requires financial records of a business to be kept for at least seven years after the transactions covered by the records are complete and Section 535 of the Fair Work Act 2009 (Cth) requires employers to make and keep employee records for seven years.

In a litigious context, it is an offence to knowingly destroy a document or any thing that is or may be required in evidence in a proceeding in the federal jurisdiction with the intention of preventing it from being used in the proceeding.[15] Similar offences exist in most jurisdictions.[16] In each jurisdiction, the terms of relevant provisions are generally broad enough to capture ESI.

It is also an offence to engage in conduct that results in the concealment, destruction, mutilation or alteration of a book relating to any matter that the Australian Securities and Investments Commission (ASIC) is investigating or is about to investigate.[17] Similar provisions exist with respect to ASIC, the Australian Prudential Regulation Authority and the Commissioner of Taxation in the Superannuation Industry (Supervision) Act 1993 (Cth).[18]

In addition to these statutory provisions, at common law, destruction of documents prior to the commencement of litigation may attract a sanction if it amounts to an attempt to pervert the course of justice or contempt of court.[19] Common law principles also provide that, where a party has destroyed documents before the commencement of the proceeding to the prejudice of the party alleging, the court may draw an adverse inference.[20]

As such, if it is known or reasonably anticipated that any regulator is about to commence an investigation or that a third party is about to commence litigation, all reasonable steps should be taken to preserve information that might be relevant to the regulator's investigation or the anticipated proceedings. This is commonly referred to as instituting a 'legal hold'.

(2009) 29 VR 123; *Chaudhary v. Bandicoot Group Pty Ltd (No 2)* [2018] FCA 420, [38]; *Global Investments Ltd v. Babcock & Brown Global Investments Management Pty Ltd*; and *DIF III – Global Co-Investment Fund LP v. BBLP LLC* [2017] NSWSC 729, [73].

15 Crimes Act 1914 (Cth) s 39.

16 See, e.g., Crimes Act 1958 (Vic) ss 254-5; Crimes Act 1900 (NSW) s 317; Criminal Code 1899 (Qld) s 129; Criminal Law Consolidation Act 1935 (SA) s 243; Criminal Code Act Compilation Act 1913 (WA) s 132; Criminal Code Act 1924 (TAS) s 99; Criminal Code Act 1983 (NT) s 102.

17 Australian Securities and Investments Commission Act 2001 (Cth) s 67.

18 See Superannuation Industry (Supervision) Act 1993 (Cth) s 286.

19 *British American Tobacco Australia Services v. Cowell* [2002] VSCA 197, [175]; *Palavi v. Radio 2UE Sydney Pty Ltd* [2011] NSWCA 264, [174-6].

20 *Moody Kiddell & Partners Pty Ltd v. Arkell* [2013] FCA 1066, [26].

While intention is key to the applicable offences, because the terms of the offences are broad (e.g., relating to anything that 'may be required in evidence'), there is a risk that the threshold will be satisfied where an individual or organisation considers that a matter, if known to a regulator or third party, might have a reasonable likelihood of being investigated or litigated (although there has been no judicial consideration of this point). In these situations, it may also be prudent to institute a legal hold to retain potentially relevant documents even if, in the case of a regulatory matter, the organisation is unable to itself determine whether a breach has occurred.

iii Sanctions

In the federal jurisdiction, the offence of destroying evidence can attract a maximum penalty of up to five years' imprisonment or a fine of up to A$300. For corporations, the maximum penalty available is A$1,500.[21] In New South Wales, the equivalent offence can attract a maximum penalty of up to 10 years' imprisonment for individuals and A$220,000 for corporations.[22]

A person who attempts to pervert the course of justice may also be liable to imprisonment. For example, in the federal jurisdiction, a person may be imprisoned for up to 10 years or be fined up to A$10,500. For corporations, the maximum penalty available is A$52,500.[23] In New South Wales, penalties may be up to 14 years' imprisonment for individuals and a fine of A$220,000 for corporations.[24]

IV REQUESTS AND SCOPE

In all jurisdictions, discovery is managed by the different case management systems in operation in each court, and parties (and their lawyers) are under a duty to assist the court to facilitate the just resolution of disputes as quickly, inexpensively and efficiently as possible.[25] However, the proliferation of ESI has magnified the complexity and cost of document production, often accounting for a large portion of the total cost of litigious or regulatory matters.

In practice, this means that courts encourage parties to limit the scope of discovery and disclosure requests. For example, discovery in the Federal Court is permitted only with the court's leave and will generally only be ordered if a party can demonstrate that it will facilitate the just resolution of the proceeding as quickly, inexpensively and efficiently as possible.[26]

21 Crimes Act 1914 (Cth) ss 4B, 39. Note that s 4B concerns pecuniary penalties applicable to natural persons and bodies corporate.

22 Crimes Act 1900 (NSW) s 317; Crimes (Sentencing Procedure) Act 1999 (NSW) ss 16–17.

23 Crimes Act 1914 (Cth) ss 4B, 43. Note that s 4B concerns pecuniary penalties applicable to natural persons and bodies corporate.

24 See Crimes Act 1900 (NSW) s 319.

25 For Federal Court proceedings, see Federal Court of Australia Act 1976 (Cth) ss 37(M)–(37M-P); for Victorian Court proceedings, see Civil Procedure Act 2010 (Vic) Part 2.3, which are discussed at s 2.4(a); for NSW proceedings, see Civil Procedure Act 2005 (NSW) ss 56–60; for Queensland proceedings, see Uniform Civil Procedure Rules 1999 (Qld) r 5; and for WA proceedings, see Rules of the Supreme Court 1971 (WA) r 1.4B.

26 See Federal Court Rules 2011 (Cth) r 20.11. Also note that the Court can give directions under r 5.04 defining the issues through pleadings or otherwise (Item 1) and regarding discovery and inspection generally (Item 10).

In all jurisdictions, courts require or encourage parties to meet and agree upon a discovery plan and document management protocol to deal with ESI. This means that litigants must undertake strategic thinking at the outset, analysing the potential cost of e-discovery, the options for controlling those costs and the process that best achieves proportionality. This is accounted for in a substantial body of practice notes in which the federal, state and territory courts provide guidance on court procedures and rules relating to discovery.

By way of example, the Federal Court specifies the following in the GPN-TECH:

a Before the court can consider making an order for electronic discovery, 'the parties will be expected to have discussed and agreed upon a practical and cost-effective discovery plan having regard to the issues in dispute and the likely number, nature and significance of the documents that might be discoverable'.[27]

b '[A]ny discovery plan and document management protocol considered by the parties must be proportionate to the nature, size and complexity of the case and should not amount to an unreasonable economic or administrative burden on the parties or the Court'.[28]

c The Court is developing a template standard document management protocol to summarise 'the terms under which information may be electronically exchanged between parties'.[29] The protocol may also include information in relation to 'reviewing and processing documents, including what methods may be used, such as keyword searches, predictive code, de-duplication of documents and email threading'[30] (some of these methods are discussed further in Section V.i). The standard document management protocol has not yet been finalised but current practice is to use the default document management protocol formulated in accordance with a Federal Court practice note that preceded the GPN-TECH.[31]

There are two main types of discovery in Australia:

a 'general' or 'standard' discovery and disclosure where a party, after reasonable searching, discovers or discloses documents in its possession, custody or power that are 'directly relevant' to the issues in dispute; or

b discovery or disclosure that is broader or narrower in scope, such as discovery or disclosure limited to categories of documents, with the categories agreed by the parties, or ordered by the court in the absence of agreement.

In practice, a party must only give discovery of documents that are found as a result of a reasonable search. When considering what constitutes a reasonable search, a party must have regard to:

a the nature and complexity of the proceeding;

b the number of documents involved;

27 GPN-TECH, para 3.3(a).

28 ibid., para 3.5.

29 ibid,. para 3.6.

30 ibid., para 3.8. Noting that parties may agree to use a different document management protocol (DMP). However, parties must understand the time and cost implications of any DMP they agree to, and subsequently, persuade the court to impose: *MHG Plastics Industries Pty Ltd v. Quality Assurance Services Pty Ltd* [2004] FCA 105.

31 See Federal Court of Australia, Practice Note CM6 (which is no longer in force) and Federal Court of Australia, Default Document Management Protocol.

c the ease and cost of retrieving a document;
d the significance of any document likely to be found; and
e any other relevant matter.[32]

In the context of ESI, this will include considering where the documents are located or held, how they are stored and how they may be retrieved.

A further issue that may arise when discovering ESI is what metadata associated with documents should be discovered. Metadata normally attaches to files when they are in 'native format' (the original, default or proprietary file format that an application reads in); however, discovery by electronic exchange is usually by way of foreign formats (e.g., PDFs, which are often referred to as images). In practice, while parties are not generally required to produce documents in their native format, it is common for some metadata associated with a document (file metadata) and metadata associated with the system the file was extracted from (system metadata) to be processed and exchanged alongside the PDF image of a document. For example, it is usually expected that at least the document date, title, email subject and email parties will be exchanged. The scope of metadata required to be produced will depend on the protocols established (and mutually agreed) between the parties.[33]

Courts can also compel the disclosure of metadata or native documents if the content of the metadata associated with the relevant documents is relevant to the issues in dispute.[34] For instance, the parties may disagree on:

a which record is the final version of a document;
b when an email was sent or received;
c whether a document was copied or modified; or
d who wrote and commented on a document.[35]

In a regulatory context, Australian regulators are increasingly requesting that native files and metadata be provided as part of document productions.

V REVIEW AND PRODUCTION

i Advanced analytical tools

Australian law firms and document review providers have been utilising advanced analytical tools for several years and there are a number of different technologies that can be used to create efficiencies in the document review process. Technology-assisted review (TAR) ranges from

32 See Federal Court Rules 2011 (Cth) r 20.14(3); Supreme Court (General Civil Procedure) Rules 2015 (Vic) reg 29.01(5); Magistrates' Court General Civil Procedure Rules 2010 (Vic) reg 29.01(1).

33 See, e.g., Supreme Court of New South Wales, Practice Note SC Gen 7: Use of Technology, 9 July 2008, para 12; Supreme Court of New South Wales Equity Division, Practice Note SC Eq 3: Commercial List and Technology and Construction List, 10 December 2008; Supreme Court of Queensland, Practice Direction No. 10 of 2011: Use of Technology for the Efficient Management of Documents in Litigation, 22 November 2011.

34 See, e.g., *Jarra Creek Central Packing Shed Pty Ltd v. Amcor Limited* [2006] FCA 1802 (application for discovery of nine fields of metadata relating to de-duplication fields denied as information found not to be necessary).

35 See Michael Legg and Lara Dopson, 'Discovery in the Information Age – The Interaction of ESI, Cloud Computing and Social Media with Discovery, Depositions and Privilege' (Research Paper No. 2012-11, University of New South Wales Faculty of Law Research Series, May 2012) 11.

less sophisticated tools (e.g., using key word searches to limit potentially relevant documents) to machine learning processes (e.g., identifying documents that may be discoverable based on a small subset of material that has been classified as discoverable by a lawyer, often referred to as predictive coding).

In most jurisdictions, legislation provides that the overarching purpose of civil practice and procedure provisions is to facilitate the just resolution of disputes as quickly, inexpensively and efficiently as possible (see Section IV).[36] Consistent with this purpose, courts in most jurisdictions promote and encourage the use of technology in the discovery process to facilitate efficiency. For example, the Federal Court has indicated a general willingness to utilise technology in the litigation process, stating that it will have an 'open mind' when it comes to rapidly changing technologies to assist in understanding key documents and minimising the document review process'.[37] The Court's practice direction implicitly endorses the use of predictive coding if both parties agree, suggesting that document management protocols should set out the parties' agreement with respect to reviewing and processing documents, including methods of review such as predictive coding.[38]

In 2016, the Victorian Supreme Court considered the use of predictive coding in a case involving 1.4 million documents that were identified as potentially relevant to a proceeding. The Court noted that traditional manual discovery was not likely to be cost-effective or proportionate and asked a 'special referee' to advise as to an appropriate process to adopt for discovery. The Court ultimately approved the special referee's recommendation to use predictive coding.[39] While there is scant judicial consideration of predictive coding in Australia, further developments are expected in this area as the technology becomes more sophisticated and courts seek to promote efficiency.

In any case, parties should disclose and agree to the use of any advanced analytics as part of the general obligation to 'meet and confer' and develop a protocol or plan for the exchange of ESI prior to commencing the discovery exercise (as discussed in Section IV). The Federal Court, ACT Supreme Court, Queensland Supreme Court, South Australian Supreme Court and Victorian Supreme Court rules and practice notes contemplate that the protocol should address the process for search and review of documents, including what methods might be used in that process.[40] Following the aforementioned case, of all the jurisdictions, the Victorian Supreme Court has dealt most comprehensively with the use of TAR. Practice Note SC Gen 5, Technology in Civil Litigation goes so far as stating that:

> *In larger cases, technology assisted review will ordinarily be an accepted method of conducting a reasonable search in accordance with the Rules of Court. It will often be an effective method of conducting discovery where there are a large number of Electronic Documents to be searched and the costs of manually searching the documents may not be reasonable and proportionate. In such cases, the Court may order discovery by technology assisted review, whether or not it is consented to by the parties.*

36 See, e.g., Federal Court of Australia Act 1976 (Cth) ss 37M-P; Civil Procedure Act 2010 (Vic) ss 7–27; Civil Procedure Act 2005 (NSW) ss 56–60; Uniform Civil Procedure Rules 1999 (Qld) r 5; and Rules of the Supreme Court 1971 (WA) ord 1, r 4B.

37 See Federal Court of Australia, Technology and the Court Practice Note (GPN-TECH), 25 October 2016, para 2.7(c).

38 ibid., para 3.8.

39 *McDonnell Dowell Constructors (Aust) Pty Ltd v. Santam Ltd (No 1)* (2016) 51 VR 421.

40 See GPN-TECH, para 3.8; Supreme Court of Victoria, Practice Note SC Gen 5: Technology in Civil Litigation (first revision), 29 June 2018, para 8.7.

The Practice Note goes on to discuss possible systems that might be used and referred to in such a protocol, including:

a a continuous active learning protocol (using a constantly changing body of documents that are used to train the TAR algorithm);

b a simple active learning protocol (using statistical samples, including control sets or random samples, etc.); and

c a simple passive learning protocol (using other recognised statistical methods).[41]

Despite positive developments in the use of TAR in discovery, because approaches in jurisdictions may differ, caution should be exercised before assuming that its use in the search and review process will be acceptable without express judicial consent. Parties should consult relevant practice notes and court rules. While the use of commonly used technology review tools (such as key word searches and deduplication) will generally be acceptable with agreement between the parties, it may prudent to tread more carefully with respect to more advanced tools such as predictive coding. Similarly, when producing documents to a regulator, the use of TAR (including less sophisticated tools such as key word searches) should be discussed and agreed to with the regulator.

ii Privilege and other concerns that may arise during production

A party is not required to produce a document that is privileged.[42] However, if a party discloses a privileged document to a third party, that party may be taken to have waived privilege if the disclosure of the document to the third party is inconsistent with the maintenance of the confidentiality that the privilege is intended to protect.[43]

Inadvertent disclosure of privileged information is an increasing risk as the volume of electronic documents to review and consider increases. However, inadvertent disclosure of privileged information will not always amount to waiver, particularly if it occurs during a court-ordered process (such as discovery), and the party acts promptly upon realising their error.[44] Australian legal practitioners also have an ethical obligation not to misuse documents that have been inadvertently disclosed by another party.[45] Accordingly, in *Expense Reduction v. Armstrong*,[46] the High Court determined that privilege had not been waived in documents that were inadvertently included in a list of documents and produced electronically on disks.[47]

41 Supreme Court of Victoria, Practice Note SC Gen 5: Technology in Civil Litigation (first revision), 29 June 2018, para 8.9.

42 See Federal Court Rules 2011 (Cth) r 20.02; Supreme Court (General Civil Procedure) Rules 2015 (Vic) reg 32.02. The Court may inspect a document over which a party has made a claim for privilege (or objects to production on other grounds) in order to determine the validity of the claim (or objection): see, e.g., Supreme Court (General Civil Procedure) Rules 2015 (Vic) reg 29.13.

43 *Expense Reduction Analysts Group Pty Ltd v. Armstrong Strategic Management and Marketing Pty Ltd* [2013] HCA 46, [30]-[32]; *Mann v. Carnell* (1999) 201 CLR 1; [1999] HCA 66 at [29].

44 *Expense Reduction Analysts Group Pty Ltd v. Armstrong Strategic Management and Marketing Pty Ltd* [2013] HCA 46, [43], [49].

45 Legal Profession Uniform General Rules 2015 (NSW) r 31.

46 (2013) 250 CLR 303.

47 ibid., 324 [63].

However, waiver will be imputed when the actions of a party are plainly inconsistent with the maintenance of the confidentiality of which the privilege is intended to protect.[48] This means that electronic documents must be reviewed diligently to mitigate the risk of inadvertent disclosure and claims of imputed waiver.[49]

In the context of large amounts of ESI, a diligent review of all materials for privilege can be challenging, and sampling is a method that has been used occasionally in different jurisdictions to determine the validity of claims of privilege. For example, in *Traderight (NSW) Pty Ltd v. Bank of Queensland Ltd (No. 16)*,[50] a privilege dispute involving 1,061 documents, the judge reviewed a sample of 30 documents and upon finding that a handful of them were arguably not privileged, dismissed the plaintiff's motion.

In some jurisdictions,[51] as part of a broader discovery plan, parties are required to agree upon the treatment of privileged documents (including any arrangements to claw back documents where inadvertent disclosure occurs).

Aside from privilege, a party does not have a general right to redact documents on the basis of irrelevance or confidentiality.[52] In some circumstances, commercially sensitive information, confidential information or personal information (see Section VI) may be redacted. In the Federal Court, a party must seek agreement from the other party or relief from the Court before redacting a document that it is otherwise required to be produced.[53] However, in some jurisdictions (e.g., in the Supreme Court of Victoria), a party can redact documents on a basis other than privilege if it can justify the redactions.[54] If a dispute arises about the appropriateness of the redactions, the Court has the power to inspect the discovered documents in unredacted form.[55]

48 ibid., 31 [30].

49 *GT Corp Pty Ltd v. Amare Safety Pty Ltd* [2007] VSC 123 [8]-12]; *LMI Australasia v. Baulderstone Hornibrook* [2000] NSWSC 1066 [21].

50 [2013] NSWSC 418.

51 See, e.g., ACT Supreme Court, Practice Direction No. 3 of 2018: Court Technology, 1 January 2019, para 14-5 provides that parties should agree upon a 'discovery plan' where discovery involves more than 500 documents; Supreme Court of Victoria, Practice Note SC Gen 5: Technology in Civil Litigation (first revision), 29 June 2018, paras 8.3–4 provide that where discovery is likely to be more than 500 documents, parties are expected to agree on an effective discovery plan. Meanwhile, in NSW, parties are required to meet and confer to consider whether ESI is to be discovered on an agreed without prejudiced basis: Supreme Court of New South Wales, Practice Note SC Gen 7: Use of Technology, 9 July 2018, para 12.

52 *Schütz Australia Pty Ltd v. VIP Plastic Packaging Pty Ltd* (No 18) [2013] FCA 407 [25] (McKerracher J), citing *Gray v. Associated Book Publishers (Aust) Pty Ltd* [2002] FCA 1045 [14]-[15] (Branson J). In *Science Research Council v. Nasse* [1980] AC 1028, Lord Wilberforce stated at 1065, 'There is no principle in English law by which documents are protected from discovery by reason of confidentiality alone.' This statement was cited by Spender J in *Mackay Sugar Co-operative Limited v. CSR Limited* (1996) 137 ALR 183, 187.

53 *Schütz Australia Pty Ltd v. VIP Plastic Packaging Pty Ltd (No 18)* [2013] FCA 407 [25] (McKerracher J), citing *Gray v. Associated Book Publishers (Aust) Pty Ltd* [2002] FCA 1045 [14]-[15] (Branson J).

54 *Octagon Inc v. Lleyton Glynn Hewitt & Another* [2011] VSC 373 at [32].

55 Supreme Court (General Civil Procedure) Rules 2015 (Vic) regs 29.11; 29.13 (in relation to documents redacted for confidentiality); Evidence Act 2008 (Vic) s 133.

iii Time frames for discovery

Discovery generally occurs after the close of pleadings (that is, after the filing and service of a statement of claim, defence and any reply, counterclaim or defence to counterclaim).[56] Although court orders for discovery are common, as noted in Section IV, not all courts permit discovery by way of right.

Once an order for discovery is made, a party must serve on the requesting party a list of documents within the period specified under the rules (often within 28 days), or within such other period as the court order may provide.[57]

iv Challenging discovery

If a party does not comply with a court order for discovery, another party may apply for an order (1) that a step in the proceeding be taken within a specified time, (2) that the proceeding be stayed or dismissed in the case of a defaulting applicant, or (3) giving judgment against a defaulting respondent. The court may make any order that it considers appropriate in the interests of justice, including orders punishing a party for contempt.[58]

The Federal Court has broad powers to address non-compliance with orders for discovery and may make orders that:

a dismiss the proceeding in whole or part;
b strike out, amend or limit any part of a party's claim or defence;
c disallow or reject any evidence;
d award costs against a party; or
e order that costs awarded against a party are to be assessed on an indemnity basis or otherwise.[59]

This is reflective of the approach taken in other jurisdictions, which all provide that a court may make a remedial order either under the relevant procedural rules or in its inherent jurisdiction.[60]

VI PRIVACY ISSUES

Under privacy laws, certain organisations have obligations not to use or disclose personal information for a purpose other than the purpose for which it was collected, unless an

56 Note that Federal Court Rules 2011 (Cth) r 20.13 provides that a party may not apply to court for an order for discovery until 14 days after all respondents have filed a defence or an affidavit in response to the affidavit accompanying an originating application; for the Victorian Courts, see Supreme Court (General Civil Procedure) Rules 2015 (Vic) reg 29.02; Magistrates' Court General Civil Procedure Rules 2010 (Vic) reg 29.02(1).

57 See, e.g., Uniform Civil Procedure Rules 2005 (NSW) r 21.3(3). Meanwhile in Victoria, discovery of documents shall be made within 42 days of service of the notice: Victorian Supreme Court Rules 2015, reg 29.03.

58 Federal Court Rules 2011 (Cth) rr 5.22, 5.23.

59 See Federal Court of Australia Act 1976 (Cth) s 37P.

60 See, e.g., Civil Procedure Act 2010 (Vic) s 56, Civil Procedure Act 2005 (NSW) s 61; Northern Territory of Australia Supreme Court Rules 2007 (NT) r 24.05.

exception applies.[61] For example, where the individual concerned has consented to the use or disclosure of the information or the use or disclosure is required under an Australian law, or court or tribunal order.[62]

For the purposes of these laws, personal information includes an individual's name, signature, address, email address, telephone number, date of birth, medical or other records and commentary or opinion about that person.[63]

It is important to be mindful of privacy obligations when undertaking discovery, particularly of ESI. For example, copies of emails and their attachments may contain personal information in the form of the sender's and recipient's names and email addresses.

The use and disclosure of personal information is permitted where an organisation is 'required' under an Australian law or court or tribunal order to handle information in a particular way and 'cannot choose to act differently'.[64] Accordingly, if a court has made an order for discovery that requires disclosure of documents, the disclosure of documents containing personal information in compliance with this order is permitted by the Privacy Act 1988 (Cth) (the Privacy Act).

However, careful attention should be given to the terms of the order. If an order is framed as requiring discovery of information about certain matters, documents that contain both relevant information and personal information might require a more cautious approach to determine if the personal information is truly covered by the order. If the order is expressed to cover documents, parties may still be able to mask irrelevant personal information contained in the relevant documents but, before doing so, they should consider the procedural rules in the relevant jurisdiction as, generally, parties do not have a right to redact documents purely for irrelevance. For example, in *Gray v. Associated Book Publishers (Aust) Pty Ltd*,[65] the respondents had produced for inspection a number of documents that had been masked on the basis that the respondents owed an obligation of confidentiality to third parties. The Federal Court ordered that the respondents produce unmasked copies of the documents and suggested that the respondents should have first obtained the applicant's agreement to the masking of the portions of their discovered documents, or otherwise sought relief from the Court. Of relevance to the Court's decision was that the information about the third parties 'might throw light' on questions relevant to the applicant's claims. In coming to this conclusion, the court noted that:

> *A private right of confidentiality in documents may be taken into account in considering whether to order discovery and inspection, although it is right to say that the fact that documents have that character is not usually itself a sufficient reason to deny discovery . . . When a document is shown to be confidential the Courts must balance the effect of its disclosure and of it being withheld from a party to litigation.*[66]

---

61 See Australian Privacy Principles (APP) para 6; Privacy Act 1988 (Cth), noting that some organisations, such as certain types of small businesses, are exempt from compliance with the Privacy Act 1988 (Cth).

62 See APP paras 6.1(a), 6.2(b).

63 See Privacy Act 1988 (Cth) s 6 and the Australian Privacy Principle guidelines issued by the Office of the Australian Information Commissioner (the APP Guidelines) at [B.85 to B.90] (https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/).

64 APP Guidelines (n 63) [B.129].

65 [2002] FCA 1045.

66 ibid., [18] (Justice Branson citing with approval the passage from Justice Kiefel in *Index Group of Companies Pty Ltd v. Nolan* [2002] FCA 608 at [8]).

Parties may also disclose information in the context of anticipated or actual proceedings without the existence of a court order. This may be acceptable under the Privacy Act if the disclosure is (1) reasonably necessary for establishing, exercising or defending a legal or equitable claim, or (2) reasonably necessary for confidential alternative dispute resolution processes.[67]

The 'reasonably necessary' test is an objective test: whether a reasonable person who is properly informed would agree that the use or disclosure is reasonable in the circumstances. It is the responsibility of the entity disclosing the information to be able to justify that the particular use or disclosure is reasonably necessary.[68] The collection, use or disclosure of personal information is unlikely to be considered necessary where it is merely helpful, desirable or convenient.[69]

When disclosing in reliance on these exceptions without a court order, parties should consider whether documents (while relevant themselves) contain any irrelevant personal information (and whether that information must be redacted before being disclosed). It is important to consider whether the disclosure of all the personal information contained in any particular document is 'reasonably necessary' in the circumstances. Redactions may be necessary if that test cannot be satisfied.

VII OUTLOOK AND CONCLUSIONS

It is likely that e-discovery and the use of TAR in Australia will continue on its current trajectory to be a readily accepted and utilised aspect of conducting litigation and regulatory matters. Australian regulators are becoming more innovative and are increasingly investing in technology to assist with their own review of large document volumes produced to them in response to regulatory notices. Following the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in February 2019, which involved significant productions to that Commission in short time frames, there has been an increase in regulatory requests and the imposition of stricter requirements around document production formats and timelines.

In the coming years, revised guidance from courts on practices for review and production of documents can also be expected. For example, the New South Wales Supreme Court's Practice Note SC Gen 7 on the use of technology has not been updated since 2008.

67 Privacy Act 1988 (Cth) s 16A.

68 APP Guidelines (n 63) [B.108], [6.61].

69 APP Guidelines (n 63) [C.25]. The draft of these guidelines explained that it would be difficult for an APP entity to be satisfied that disclosure was reasonably necessary merely at the request of a third party without a court order. This does not appear in the final APP Guidelines.

Chapter 3

BELGIUM

Flip Petillion, Jan Janssen, Diégo Noesen and Alexander Heirwegh[1]

I OVERVIEW

Unlike in the United States or other jurisdictions where proceedings are conducted on an accusatory basis,[2] the Belgian legal system – comparable to most civil law systems – is of an inquisitorial nature. This means that the claimant has the principal obligation to produce the necessary evidence to prove its allegations. This principle is laid down in Article 870 of the Belgian Judicial Code. The responsibility and costs for providing the necessary evidence in a case is therefore borne by the accusing party.

In Belgium, the parties are considered the directors of the proceedings, with the court playing a more passive role.[3] However, if a claimant aims to obtain the production of specific evidence (documents) that it cannot reasonably acquire and that is under the control of the opposing party, it may request the court to order the production of this evidence under its possession.[4] As a result, the court may acquire a much more central and active position in the collection of information relevant to the proceedings. The Belgian system clearly differs from common law systems, where the court fulfils a secondary role in the collection and exchange of information and where the parties are obligated to exchange all information related to the proceedings under their control, irrespective of this information being advantageous or detrimental to their case.

It follows that the discovery procedure is not automatic, nor a prerequisite for proceedings. Discovery – within the meaning of collecting and handing over relevant information to the opposing party – is dependent upon a specific request by a party or a court order, or both. The court can order that a party to the litigation, or even a third party, produces a specific piece of evidence when there are important, precise and corresponding presumptions that the party has such evidence in its possession or control and that the evidence can prove a relevant fact.[5]

Although the production of documents can be ordered at the court's initiative (*sua sponte*),[6] it is recommended that parties issue a request for the production of documents and ask that the order is accompanied by a penalty payment in the case of non-compliance.

---

1 Flip Petillion is the founder and managing partner, Jan Janssen and Diégo Noesen are senior associates, and Alexander Heirwegh is an associate, at Petillion.

2 U.S. Federal Rules of Civil Procedure 16, 26 and 34.

3 Brussels Court of Appeal, 17 December 2008, 2008/AR/90.

4 Article 871 Judicial Code.

5 Article 877 Judicial Code.

6 S. Stijns, 'De overlegging van stukken in het Gerechtelijk Wetboek', *Jur. Falc.* 1984–85, p. 209; J. Van Compernolle, 'La production forcée de documents dans le Code judiciaire', *Ann. Dr. Louvain* 1981, p. 92.

Penalty payments may only be issued at a party's request.[7] In any event, if a party or third party illegitimately refuses to produce documents, it may be condemned to pay damages at the request of the harmed party.[8] The destruction, alteration or concealment of evidence in contravention of an order to produce documents may also be sanctioned by imprisonment or fines, or both.[9] Parties are prohibited from withholding decisive evidence. A case may be reopened following the closing of the debates, before, and even after, the issuing of a decision, if a party can demonstrate that the other party withheld key information.[10]

While an order to produce documents can be compared to discovery actions in the United States, the order first requires a careful balancing of the conflicting interests and is limited to specific documents and information that are important for the decision. A party may therefore not request that an adverse party or an (in)directly involved third party produces all documents in relation to, for example, certain transactions, so that it may potentially find an element that is disadvantageous to the adverse party.[11] These 'fishing expeditions' are not allowed in Belgian legal proceedings. The court may examine the importance and relevance of the specific piece of evidence, the legitimacy of the adverse party's request for dismissal, the appropriateness of the 'production order', and the stage of the proceedings in which the order is requested.[12]

If a judge wants to order a third party to produce documents, it must first invite the third party to submit the documents voluntarily and make potential reservations.[13] Professional secrecy obligations may, for instance, prevent the third party from disclosing the documents. Claiming that the documents have been destroyed or no longer exist will not necessarily suffice as an excuse not to produce the documents. Precedent exists where a judge appointed experts to investigate the veracity of this type of claim.[14]

An order to produce documents remains a purely discretionary measure.[15] The order cannot be appealed.[16] Only related measures, such as a penalty payment, are open to appeal.[17]

---

7 Article 1385 *bis* Judicial Code, by virtue of which penalty payments may only be imposed on an adverse party to the proceedings. Hence, it would not be possible to accompany an order to produce evidence targeted against a third party with a penalty payment without making the third party a party to the proceedings. However, case law and legal doctrine seem to accept that a penalty payment may be imposed on a third party after the third party was heard (Civ. Liège 14 February 1991, *JLMB* 1991, 975; Civ. Liège (Réf.) 2 July 1980, *JL* 1980, 241, Commentary de Leval; Civ. Huy 30 December 1981, *JL* 1982, 137, Commentary de Leval; Comm. Liège 3 March 1993, *JLMB* 1993, 1274; A. Kohl, 'Astreinte et production de documents dans le cadre de la fixation du montant d'une pension alimentaire', *JLMB* 1991, p. 975; J. Van Compernolle, 'La production forcée de documents dans le Code judiciaire', *Ann. Dr. Louvain* 1981, p. 104; *A contrario*: S. Stijns, 'De overlegging van stukken in het Gerechtelijk Wetboek', *Jur. Falc.* 1984–85, p. 219).

8 Article 882 Judicial Code; Cass. 7 April 2014, No. F-20140407-1 (S.12.0121.N).

9 Article 495 *bis* Judicial Code.

10 Article 772 and following Judicial Code; Article 1133, 2° Judicial Code.

11 Brussels Court of First Instance, 3 February 2011, *TRV* 2011 ed. 3, 199.

12 Brussels Commercial Court, 24 February 2017, A/14/50711, *IRDI* 2017 ed. 3, 221.

13 Article 878 Judicial Code.

14 Bruges (5th Chamber), 23 April 2010, *TGR-TWVR* 2010/4, 255.

15 Cass. 17 June 2004, C.02.0503.N; Cass. 14 December 1995, *RW* 1996-97, 198.

16 Article 880 *in fine* Judicial Code; Cass. (1st Chamber) AR C.13.0014.F, 11 September 2014 (BNP Paribas / Banco Monte Paschi Belgio), *Arr. Cass.* 2014/9, 1837; *JT* 2015, No. 6596, 239, Commentary Baetens-Spetschinsky, M; *JLMB* 2016/19, 872; *Pas.* 2014/9, 1817, concl. Henkes, A.

17 Antwerp Court of Appeal (3rd Chamber), 1 June 2005, *P&B* 2005/5, 233.

The order can be based on significant, defined and consistent presumptions.[18] Despite the requirement that presumptions must be consistent, case law accepts that a single presumption may suffice.[19] The law requires that the document identified in the order to produce be relevant, though not necessarily decisive, for the decision on the merits.[20]

The law makes no distinction between the disclosure of traditional documents and the disclosure of electronically stored information (ESI) and no specific law on the disclosure of ESI exists. For a document to be targeted in an order to produce, it suffices that the document is stored on a material data carrier.[21] However, the requested document must exist on the data carrier. If a document must be created from the data set and requires the performance of a service before it can be generated, a request to produce the document may not fall under the rules for documentary discovery.[22] Some courts adopt a lenient approach[23] and legal doctrine advocates that requests for documentary disclosure should be granted if the creation of the document is extremely easy.[24] When more complex handling is required to extract relevant information from large data sets, an investigation by a court-appointed independent expert will be more appropriate in most cases than the disclosure of bulk information.

When requesting the disclosure of ESI, it may also be necessary to ask for ancillary measures. ESI is often password protected or stored in file formats that may not be readable without specific software licences. Judges may order measures, such as the communication of passwords or mandatory printouts in readable format, to ensure effective access to ESI.[25]

Apart from the general procedure on the production of evidence, specific 'discovery actions' exist in the context of individual fields of law.

In intellectual property (IP) cases, the holder of a prima facie valid IP right may request the *ex parte* appointment of an expert to describe all the (physical and electronic) documents, objects, elements and processes that may demonstrate the alleged counterfeit, its origin and its extent.[26] Apart from descriptive measures, this counterfeit seizure may also include conservative measures, such as the seizure of litigious goods, documents and materials, and the withdrawal of the goods from distribution channels. Before awarding *ex parte* conservative measures, the judge will balance all relevant interests and examine whether the IP infringement cannot be reasonably disputed. After having determined an IP infringement,

18 Article 877 Judicial Code.

19 Cass. (1st Chamber) AR C.14.0512.F, 16 October 2015 (BMW Belgium Luxembourg / G. business services), *Arr. Cass.* 2015/10, 2386; *Pas.* 2015/10, 2367, concl. Leclercq, J.; *RW* 2016-17/25, 991.

20 Article 877 Judicial Code; Cass. (1st Chamber) AR C.14.0512.F, 16 October 2015 (BMW Belgium Luxembourg / G. business services), *Arr. Cass.* 2015/10, 2386; Pas. 2015/10, 2367, concl. Leclercq, J.; *RW* 2016–17/25, 991.

21 J. Laenens, D. Scheers, P. Thiriar, S. Rutten and B. Vanlerberghe, *Handboek Gerechtelijk Recht*, Antwerp, Intersentia, 2016, 580, No. 1365.

22 See Mons, 1 October 2002, *JT* 2002, 815.

23 See Pres. Civil Court of Ghent, 27 May 2005, PB 2006, 76; Court of Ghent, 29 June 2005, PB 2006, 78.

24 See T. Toremans, 'De overlegging van een niet-gematerialiseerd stuk op basis van de artikelen 871 en 877 Ger.W.', *P&B* 2017/5–6, 243.

25 See e.g., Labour Court of Appeal Ghent 23 June 2010, *TGR* 2011, 110; Comm. Court Namur, 29 June 1995, *RRD* 1995, 471.

26 Article 1369 *bis*/1 Judicial Code.

a judge may also order the production of all known documents and information concerning the origin and the distribution networks of the infringing goods or services upon the request of the IP right holder, as far as this measure seems justified and reasonable.[27]

In the context of national and European antitrust or state aid investigations, the Belgian Competition Authority (BCA) and European Commission may exercise their investigative powers by issuing an information request demanding the production of specific documents or by examining and copying specific (electronic) records during an inspection (see Section V).

The production of (electronic) documents may also be ordered in the context of fraud and anti-money laundering investigations conducted by the Belgian Financial Services and Markets Authority and inspections by the Belgian Tax Administration.

With regard to foreign discovery orders, Belgium is not a party to the Hague Convention of 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters.[28] However, it is a party to the Hague Convention of 1954 on Civil Procedure,[29] which mandates that a request for obtaining evidence must be sent via a letter of request through mutual consular channels. As Belgium is not a party to the Hague Convention of 1970 on the Taking of Evidence Abroad and the United States is not a party to the Hague Convention of 1954 on Civil Procedure, discovery orders issued by a United States court are treated solely on the basis of international custom. As no specific blocking statutes exist that would prohibit compliance with a foreign discovery order, a Belgian entity is generally required to comply with a US discovery order. A Belgian court would only consider prohibiting the enforcement of a foreign (including US) discovery order if it has jurisdiction to rule on the merits of the case.[30]

Within the European Union, requests for the taking of evidence in civil or commercial matters are governed by Regulation (EC) No. 1206/2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters.[31] This regulation provides for a simplified procedure of requests for the production of evidence directly between EU courts.

II YEAR IN REVIEW

The entry into force of the General Data Protection Regulation (GDPR)[32] on 25 May 2018 and the corresponding Law of 30 July 2018 on the Protection and Processing of Personal Data (the Data Protection Law)[33] introduced stricter rules on the processing of personal data in Belgium, including in relation to discovery. Although personal data (including sensitive data) may be processed and transferred in the context of determining, exercising and defending a legal claim, the discovery and production of (electronic) documents must be limited to objectively relevant personal data, which must be deleted from the moment these are no longer necessary for the legal proceedings (see Section VI).

27 Article XI. 334 Section 3 Code of Economic Law (CEL).

28 Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, 18 March 1970, 23 *U.S.T.* 2555, *T.I.A.S.* 7444, 847 *U.N.T.S.* 231.

29 Hague Convention on Civil Procedure, 1 March 1954, 4123 *U.N.T.S.* 267.

30 Brussels Court of Appeal, 21 October 2005, *TBH* 2006, 970.

31 *OJ L* 174, 1.

32 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 1.

33 BS 2018040581, 5 September 2018, 68616.

On 30 July 2018, Belgium also implemented the new EU Directive on the Protection of Trade Secrets.[34] The Law on the Protection of Trade Secrets[35] implements certain safeguards to ensure that trade secrets cannot be used or disclosed by a party, its representatives, judges, witnesses, experts or other persons taking part in the proceedings. This prohibition only applies to trade secrets included in documents that were marked as confidential by the court, either at its own initiative or upon a motivated request by a party.[36] In the context of discovery, the court may also order that access to the documents containing trade secrets is limited to certain specifically appointed persons or that a non-confidential version of those documents is drafted for all other participants in the proceedings, redacting the parts of the document containing trade secrets.[37]

In relation to criminal investigations and proceedings, the European Union has taken several initiatives with regard to cross-border access to electronic evidence. For international criminal cases beyond the European Union, the European Commission presented two sets of negotiating directives on 5 February 2019 in order to start negotiations with the United States and with the Council of Europe.[38] The negotiations aim to facilitate cross-border access by judicial authorities in criminal proceedings to electronic evidence held by an electronic communication, information society, internet domain name or IP-address service provider abroad. At the same time, an internal proposal for an EU Regulation was made to make it easier and faster for police and judicial authorities in criminal investigations or proceedings to obtain the electronic evidence they need, such as emails or documents, located on the server or the cloud of EU service providers. The proposed e-Evidence Regulation[39] introduces a European Production Order and a European Preservation Order, allowing judges to request the production or preservation of electronic evidence directly from a service provider established in another Member State, subject to safeguards regarding privacy and other fundamental rights.

The Belgian Constitutional Court issued an important decision on 23 January 2019 regarding the tensions between discovery and professional secrecy.[40] The case concerned a specific employment law[41] on the basis of which a prevention adviser could refuse access to a psychoanalytic report and associated documents to the subject of that report on the basis of professional secrecy. In other words, the law provided for an exception to the general right of access to personal data of individual data subjects. The Constitutional Court decided that

34 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, *OJ L* 157, 1.

35 Law of 30 July 2018 Regarding the Protection of Trade Secrets, BS 2018031595, 14 August 2018.

36 Article 871 *bis*, Section 1 Judicial Code.

37 Article 871 *bis*, Section 2 Judicial Code.

38 Council Decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, 5 February 2019, COM(2019) 70 final; Council Decision authorising the participation in negotiations on a second Additional Protocol to the Council of Europe Convention on Cybercrime (CETS No. 185), 5 February 2019, COM(2019) 71 final.

39 Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, 17 April 2018, COM(2018) 225 final, 2018/0108 (COD).

40 Constitutional Court, 23 January 2019, Judgment No. 2/2019, 6685.

41 Articles 32 *quinquiesdecies* and 32 *septiesdecies* of the Law of 4 August 1996 regarding the well-being of employees in the performance of their work.

this statutory provision would violate the constitution and the fundamental right to a fair trial (Article 6 of the European Convention on Human Rights) when this would preclude that a court can order the production of documents in proceedings. The Constitutional Court continued that a request for the production of documents may not be denied solely on the basis of professional secrecy and that, instead, a judge may order that the relevant documents are first handed over to the court to examine the importance of those documents for the resolution of the dispute in accordance with the right of defence. Additionally, while balancing the right of a fair trial with the right of professional secrecy, a judge may also order that certain data be anonymised or that certain parts of the documents be redacted or withheld.

III CONTROL AND PRESERVATION

The law offers no definition for the concept of control in the context of the production of ESI or other evidence. Whether a party controls ESI will be a fact-based discussion. Recent case law seems to suggest that a party must be able to obtain immediate access to the ESI for the information to be discoverable to that party. Inter-company access restrictions may render ESI that is stored on a foreign server non-discoverable, even if the party with whom discovery is sought has a regulatory obligation to preserve the information and to ensure that the information can be made available to a public authority within a short time frame.[42] Contractual purpose limitations for accessing electronic information stored on a remote server could thus shield certain data from being disclosed to parties that are not explicitly targeted in specific rules on mandatory access to information.

Establishing inter-company data storage and data access policies may seem a daunting task in view of the myriad of sector-specific regulations that exist, for example, in tax, employment and life sciences. If documents are stored off-site, tailored agreements will be required to ensure regulatory compliance by (international) business data centres.

The electronic storage of documents is generally allowed, provided that the electronic filing system guarantees their authenticity and integrity during the entire retention period. Certain documents must be kept in their original form. As such, the electronic storage of a copy may not always be sufficient. Since 2001, private agreements can carry an electronic signature, namely a combination of electronic data that can be attributed to a specific person and that demonstrates the preservation and integrity of the content of the document.[43] Without an electronic signature, the document must be preserved in its original physical form for evidentiary reasons.

The rules on the preservation of documents and data are dispersed across different pieces of legislation. Express requirements to preserve documents and sanctions for non-compliance can be found in corporate legislation, tax laws, laws on customs and excises, environmental legislation, labour laws, anti-money laundering legislation, etc. Specific rules apply in different sectors. They can be harmonised in the European Union (e.g., electronic communications traffic data, telecommunication data, financial data) or be country- or region-specific (e.g., health, construction, media data).

42 Pres. Dutch-speaking Comm. Court Brussels, 8 June 2017, *IRDI* 2017/2, 125.

43 Article 1322 Civil Code.

In the context of litigation, there is an absolute prohibition to fraudulently destroy, alter or hide evidence after disclosure has been ordered by the court. Violations are punished with imprisonment of eight days to two years and criminal fines of €208 to €8,000.[44] The nature of the evidence may give rise to higher fines and more severe punishment. For example, the wilful removal of accounting documents is punished with one month to five years' imprisonment and criminal fines of €800 to €4 million.[45] In addition, non-compliance with a court order to produce may give rise to damages and penalty payments.[46]

IV REQUESTS AND SCOPE

In litigation, requests for document production must relate to specific documents. In relation to proceedings on damages for antitrust violations, the request may relate to categories of documents that are clearly and narrowly defined.[47] The requester must convince the court that the requested documents corroborate one or more facts that are pertinent to the case.[48] Fishing expeditions are not allowed. The requirement that a party or a third party holds a pertinent document must be met for each individual document requested. Even if the court determines that a party holds certain documents under its control that are pertinent to the case, it will not automatically grant a request for the production of ESI. The court will make a discretionary appraisal of the different interests at stake, the merit of the production order, the importance of the documents, the legitimacy of the adverse party's request for dismissal and the stage in the proceedings in which the request for production was made.[49]

There is no requirement for parties to meet and confer in the context of disclosure of documents or ESI. Of course, nothing prevents parties from agreeing on voluntary models to share and access information. These agreements rarely occur in practice, but can be useful, for instance when a party intends to submit information in redacted form.

In arbitration, agreements on the taking of evidence and disclosure of ESI are more common, even though document production in domestic arbitration is often inspired by the (stringent) criteria used by local courts. Since the introduction of the new Arbitration Law in 2013, arbitrators have broad discretion in ordering document production. The Law imposes no specific rules or modalities.[50] In international arbitration, general practice accepts that parties request categories of documents, provided the category is sufficiently narrow and specific.[51] In the context of disclosure of ESI, it is not uncommon that search terms, specific individuals or searching methods are identified for the collection of relevant documents.

44 Article 495 *bis* Criminal Code of 8 June 1867.

45 Article 489 *ter* Criminal Code of 8 June 1867.

46 Article 882 Judicial Code; Article 1385 *bis* Judicial Code.

47 Article XVII.74 CEL.

48 Article 877 Judicial Code.

49 Brussels Commercial Court, 24 February 2017, A/14/50711, *IRDI* 2017 ed. 3, 221.

50 Article 1700, Section 4 Judicial Code.

51 See Articles 3 and 9 IBA Rules on the Taking of Evidence in International Arbitration, adopted by a resolution of the IBA Council 29 March 2010.

V REVIEW AND PRODUCTION

As document production in commercial litigation relates to specific documents and not to general categories of documents, the use of advanced analytical tools is not prevalent before Belgian courts. Nevertheless, these tools can be used in the framework of an expert opinion. In this event, the expert will normally make mention of the technology used when describing the report's methodology.

When requested documents are legally privileged or contain trade secrets, the party holding the documents should immediately file a motion for dismissal or request ancillary measures to preserve their confidentiality. As an order to produce cannot be appealed,[52] a party to the proceedings must object to the production of documents before the order is issued. Third parties will be invited to submit the documents voluntarily before an order is issued.[53] Potential reservations to the production of documents should be made then.

If a party or third party illegitimately refuses to produce documents, it may be condemned to pay damages upon request of the harmed party.[54] The destruction, alteration or concealment of evidence in contravention of an order to produce may also be sanctioned by imprisonment or fines, or both.[55] In addition, the order to produce may, at a party's request, be accompanied by a penalty payment in case of non-compliance. Whereas the order to produce cannot be appealed, the condemnation to damages, sanctions or penalty payment is open to appeal.[56]

Document production can also be ordered in the context of government investigations. Government authorities make use of technology-assisted review, analytics and predictive coding to facilitate the review of ESI and documents seized in the context of antitrust or other investigations.

In national antitrust investigations, the BCA will determine whether the seized documents are in scope, out of scope or subject to legal professional privilege (LPP). The selection of ESI and documents is done in the presence of the company that is subject to the investigation. The selected ESI and documents are stored in three separate repositories:

a the in-scope repository contains the documents for which the company does not challenge the collection;

b the out-of-scope repository contains the documents that the seizing authority considers relevant, but that the company considers go beyond the scope of the search warrant; and

c the LPP repository contains the documents that the company considers legally privileged and of which the privileged nature is challenged by the seizing authority.

Only the in-scope repository will be available to the investigation team. The company concerned is granted at least 10 working days to provide the authorities with a list of the documents that have been taken up in the LPP and out-of-scope repositories together with an explanation as to why the documents must be considered as privileged or out of scope.

52 Article 880 *in fine* Judicial Code; Cass. (1st Chamber) AR C.13.0014.F, 11 September 2014 (BNP Paribas / Banco Monte Paschi Belgio), *Arr. Cass.* 2014/9, 1837; *JT* 2015, No. 6596, 239, Commentary Baetens-Spetschinsky, M.; *JLMB* 2016/19, 872; *Pas*. 2014/9, 1817, concl. Henkes, A.

53 Article 878 Judicial Code.

54 Article 882 Judicial Code; Cass. 7 April 2014, No. F-20140407-1 (S.12.0121.N).

55 Article 495 *bis* Judicial Code.

56 See Antwerp Court of Appeal (3rd Chamber), 1 June 2005, *P&B* 2005/5, 233.

An officer who is not involved in the investigation will examine whether LPP applies to the individual documents in the LPP repository. The examination is done in the presence of the company concerned. The officer may ask for assistance from IT experts. If the officer determines that a document is subject to LPP, it will be deleted from the file. With respect to the out-of-scope repository, an officer working on the case will determine, on the basis the company's explanation of the document, whether the seized documents are in fact out of scope. The examination will be done in the presence of the company concerned and the officer may require the assistance of IT experts and BCA personnel. If an officer decides that the document must be added to the file, the decision is subject to appeal.[57]

In contrast to investigations by EU authorities, LPP for the Belgian authorities applies to both communications with external lawyers and communications with internal corporate counsel who are members of the Belgian Institute of Corporate Counsel.[58]

The seized documents may contain sensitive or confidential information. To preserve the confidential nature of the documents, BCA personnel are bound by professional secrecy obligations[59] and proceedings exist to keep information classified if not outweighed by reasons of public interest in enforcing antitrust laws.[60] A decision to disclose previously classified information may be appealed with the BCA.[61] Also, the production of documents seized by the BCA in court litigation is subject to strict conditions.[62]

VI PRIVACY ISSUES

Since 25 May 2018, the GDPR applies to the processing of personal data in Belgium. The provisions of the GDPR are complemented by the Data Protection Law. In most legal proceedings where the production of ESI is ordered, personal data will be retained, disclosed and transferred, and the data protection rules apply. The GDPR will apply to discovery when either the requesting or the controlling party is established in the European Union, as both the collection and the transfer of personal data are processing activities to which the GDPR applies.[63]

As a result, an assessment must be made in accordance with the GDPR as to whether (1) there is a legitimate basis for processing the (sensitive) personal data contained in the ESI for the purpose of discovery; (2) the processing is necessary and proportionate for that purpose; (3) the personal data is not retained longer than is necessary for that purpose; (4) the data subjects' rights are observed; (5) sufficient technical and organisational precautions are taken to protect the data; and (6) for foreign discovery orders, whether the principles with regard to the transfer of personal data to third countries are complied with.

For the discovery of personal data contained in ESI to be lawful, it must be based on one of the legitimate grounds set out in Articles 6 and 9 of the GDPR. The relevant legitimate bases in this regard are: consent; the need to comply with a legal obligation; the

57 Article IV.79 CEL.

58 See CJEU, C-550/07 P, 14 September 2010, *Akzo Nobel Chemicals Ltd. et al. v. European Commission*, ECLI:EU:C:2010:512; Article 5 Law of 1 March 2000 on the establishment of an Institute of Corporate Counsel.

59 Article IV.34 CEL.

60 Article IV.41(7) CEL.

61 Article IV.41(8) CEL.

62 Article XVII.77-80 CEL.

63 See Articles 2 and 3 (Material and Territorial Scope) GDPR.

overriding legitimate interest of the requestor or controller of the ESI; or the need for the establishment, exercise or defence of legal claims. As consent is generally not accepted in an employer–employee relationship and can be withdrawn at any time, it is not a recommended basis for discovery actions. Additionally, the need to comply with a legal obligation can only be invoked in the context of a production order by a national court based on Belgian law and cannot be based on a foreign legal stature or regulation.

In the context of cross-border discovery, parties therefore generally rely on their overriding legitimate interest of complying with the requirements of the litigation process to collect or disclose personal ESI. However, this legitimate interest of the parties does not automatically justify the processing of personal data for the purpose of discovery as it requires a careful balancing with the privacy interests of the data subjects concerned, taking into account the principle of proportionality, the relevance of the personal data to the litigation and the potential consequences for the data subject. As this balancing exercise also requires that adequate safeguards are put in place, parties should first consider anonymising or at least pseudonymising the personal data that is not strictly necessary for the discovery action.[64]

Specifically for ESI containing sensitive data,[65] such as data concerning health, the parties must ensure that the disclosure of this data is strictly necessary for the establishment, exercise or defence of legal claims. Otherwise, this data should be redacted or anonymised (e.g., in the form of statistical data). Due account must also be taken of other duties of confidentiality, such as professional secrecy obligations, with regard to sensitive data.

Personal correspondence, such as emails or letters, are also subject to the applicable data protection regulations and generally require the consent of both the sender and the receiver to be accessed and disclosed. Criminal sanctions apply to any person who opens or discloses personal communication without the authorisation of the persons involved.[66] With regard to employees' emails, specific rules apply. Article 128 of the Law on Electronic Communication provides that an employer may record and retain emails of its employees in the context of legal business transactions in order to prove a commercial transaction or another business communication, subject to the conditions that the persons involved are properly informed and that the data is deleted after the statute of limitations for challenging the transaction has passed. Employers must also comply with various collective labour agreements that govern privacy in the employment relationship. Collective Labour Agreement 81 concerns the monitoring of electronic online communication by employers. In this context, e-discovery actions pertaining to employee emails are only justified for the following purposes: the prevention of unlawful or defamatory facts, or facts contrary to public decency or capable of damaging the dignity of another person; the protection of the economic, trade or financial interests of the company; and bona fide compliance with the company's policies and rules for the use of online technologies.[67] In contrast to emails, personal files and documents

64 Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, Article 29 Data Protection Working Party, 11 February 2009, 00339/09/EN WP 158, p. 10.

65 Article 9.1 GDPR defines special categories of data as: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

66 Article 314 *bis* Criminal Code.

67 Article 5 Section 1, Collective Labour Agreement 81 of 26 April 2002 on the Protection of Privacy of Employees with Regard to the Monitoring of Electronic Online Communication Data, BS 2002A12699, 29 April 2002, 29490.

created and saved by an employee on his or her work computer are not considered electronic communication data and – together with the connected IDs and passwords – can be the subject of a production order in legal proceedings.[68]

For foreign production orders resulting in the transfer of electronically stored personal information to third countries outside the European Union, notably the United States, specific data protection obligations apply. Apart from transparency obligations towards the data subjects involved, the GDPR requires that there exists an adequate (i.e., equivalent) level of protection of personal data in the receiving country. This could either be based on an adequacy decision by the European Commission or on the incorporation of safeguards for the transfer of personal ESI, such as standard contractual clauses or binding corporate rules. As the United States is not deemed to have an adequate level of protection, parties must rely on these safeguards in the context of a US discovery order. The recipient in the United States could also subscribe to the EU–US Privacy Shield to warrant the protection of personal data during the discovery process. In the absence of these safeguards, a party may only transfer the personal data contained in the ESI for the purpose of discovery in a third country insofar as this is strictly necessary for the establishment, exercise or defence of legal claims.[69] However, the latter derogation cannot be used to justify the transfer of all employee files to a recipient in, for example, the United States in the anticipation of a potential legal action. The derogation only justifies a single transfer of relevant information pursuant to a threat of legal action.[70]

VII OUTLOOK AND CONCLUSIONS

Apart from initiatives on cross-border access to electronic evidence in criminal investigations and proceedings (see Section II), the European Union has also taken several steps to promote and regulate the development and application of emerging technologies, such as distributed ledger technology (blockchain) and artificial intelligence (AI).[71] Applications, such as smart contracts and next generation search algorithms, will further facilitate the (cross-border) access to and transfer of ESI necessary for legal proceedings, while at the same time enhancing safeguards for the increasingly important protection of privacy, personal data and trade secrets. Specifically in relation to antitrust and mergers, the European Commission has announced its commitment to explore the possible contribution of AI technologies to help staff review electronically stored documents originating from companies under scrutiny (technology-assisted review) and launch a study on certain use cases for data analytics applied to competition enforcement.[72]

68 Ghent Labour Court (Appeal), 23 June 2010, *TGR-TWVR* 2011, ed. 2, 110.

69 Article 49.1(e) GDPR.

70 Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, Article 29 Data Protection Working Party, 11 February 2009, 00339/09/EN WP 158, p. 13.

71 See, *inter alia*, the Declaration creating a European Blockchain Partnership, Brussels, 10 April 2018; Blockchain and the GDPR Report, European Union Blockchain Observatory and Forum, EU Thematic Report, 16 October 2018, 36; Coordinated Action Plan to Foster the Development and Use of AI in Europe, European Commission, 7 December 2018, COM(2018) 795 final; Declaration of Cooperation on Artificial Intelligence, Brussels 10 April 2018.

72 EU Commission Management Plan 2019, DG Competition, 19 December 2018, ARES(20186571012, 40.

Belgian courts become increasingly used to the handling of confidential information within proceedings. It is anticipated that the use of data rooms to exchange evidence, redaction of evidence and hearings in chambers will increase now that the EU Directive on the Protection of Trade Secrets has been implemented (see Section II). Companies and judges are also expected to make increasing use of virtual data rooms in relation to the disclosure of confidential or sensitive documents instead of the conventional physical data rooms. Reforms in the past couple of years show that the legislature is sensitive to balancing the right to privacy with the constitutional right to public hearings. Elections are due to take place in Belgium on 26 May 2019; the next Parliament will likely be invited to amend the Constitution to modernise the rules on the publication of judgments.[73] It is expected that the new rules will offer clear guidance on the redaction of confidential information.[74]

73 See Belgian Chamber of Representatives, Plenary Session of 14 February 2019, Full Report, Doc CRIV 54 PLEN 270, www.dekamer.be/www.lachambre.be, p. 63.

74 See parliamentary bill to amend the Code on Criminal Proceedings and the Judicial Code regarding the publication of judgments, 15 February 2019, Doc 54-3489/004, www.dekamer.be/www.lachambre.be, p. 5.

Chapter 4

BRAZIL

Eloy Rizzo, Danilo Orenga and Victoria Arcos[1]

I OVERVIEW

i Litigation

Brazil does not have a discovery procedure and, in the context of legal claims, is unfamiliar with the concept of electronic discovery (e-discovery) and the rules of electronically stored information (ESI). There are no laws or regulations that provide how the parties, or the judges, should behave in this scenario. In other words, Brazil, which is a civil law jurisdiction, does not provide or demand the use of discovery in legal claims. In March 2016, the new Brazilian Civil Procedure Code (CPC) entered into force after several years of discussion before the legislative branch and many new ideas – including some that were inspired by the common law system, such as the binding precedent rule – were introduced to a system that had experienced few substantial changes for decades. However, none of the new concepts had a significant impact on the evidence procedure phase.

However, this does not mean that the parties cannot decide to have their specific case processed according to the rules of discovery and ESI. The CPC provides that parties may jointly determine the procedural rules of a current or future dispute, which allows them the opportunity to use discovery and ESI as a way of gathering and producing evidence for the case. This is an opportunity that has not been used very frequently to date, not only as a result of the lack of information regarding the proceedings related to e-discovery, but mainly because judges have the final say regarding how cases are conducted and define the legal issues that must be solved by evidence production or by the analysis of the law. The courts are flooded by thousands of legal proceedings and the notion that some cases should be conducted in a special manner by the courts, as defined by the parties themselves, does not elicit the sympathy of judges, who have the power to overrule or to modify the parties' decision based on the argument that it is their responsibility to deal with all cases in a fair and equal manner. The costs related to this procedure are also an obstacle.

Regardless of legislative changes, the way that evidence is produced has not substantially changed, as the parties remain responsible for producing evidence of the facts either to use against the opposing party or to justify their own position. Electronic evidence accounts for a significant portion of the evidence that is presented to courts, especially related to business conflicts, but each party is responsible for producing the evidence, without having full access to the evidence that the opposing party has in its files. In addition, all evidence must be presented before the judge, mostly in his or her physical presence or, in the case of

1 Eloy Rizzo is a partner, and Danilo Orenga and Victoria Arcos are associates, at KLA – Koury Lopes Advogados.

technical evidence (e.g., engineering or accounting evidence), before an individual who has the competence to review it. These individuals are appointed by the judge as persons of his or her confidence, based on the individual's expertise and the quality of his or her work. Cross-examination and full access to the other party's files have no legal basis and are methods that are not commonly used by lawyers.

The official use of e-discovery in proceedings is still unlikely to be introduced, as this decision rests with the legislative branch, which is currently extremely busy dealing with corruption accusations. In addition, the use of discovery is at odds with Brazilian legal culture, which does not appear to be willing to accept that parties must be able to access each other's files.

ii Internal investigations

With regard to internal investigations, there is no specific legislation or guideline that determines how to conduct e-discovery in an investigative process. Internal (or corporate) investigations are a recent innovation, and both public authorities and the majority of organisations are not accustomed to the procedures that govern the process. Thus, lawyers and external counsel rely on international best practices to guide the investigation process.

External counsel (lawyers or forensic auditors) frequently lead or oversee internal investigations because of their expertise in evaluating facts, and, with regard to lawyers, for the legal protection afforded by attorney–client privilege.

Adapting foreign practices has resulted in cultural clashes in the conduct of internal investigations. For example, for data collection in most countries, it is advisable that when starting an investigation, a company should issue a preservation notice and obtain consent from employees prior to the collection of data from corporate devices. However, in Brazil this guidance has resulted in massive deletion of data. Another cultural clash that directly impacts e-discovery in internal investigations is the lack of comprehensive internal controls in some companies, including those that relate to backup of information and data storage capacity. The resulting lack of information has led to several inconclusive investigations.

The general approach to e-discovery in internal investigations comprises the following steps: (1) assessment of the allegation and formulation of the investigative plan; (2) evidence collection, preservation and processing; (3) electronic document review and evidence analysis; and (4) overall assessment and considerations.

Regardless of the structure of the investigative process, the better the depth and quality of the information gathered through e-discovery, the more prepared and informed the counsel is to assess the impact of the findings on a company's corporate policies, legal requirements and reputation. As the investigation is being conducted, this process may become cyclical if the assessment of certain findings leads to modifications to the investigation plan.

Despite there being no formal e-discovery procedure or recognition of ESI disclosure, in practice, e-discovery plays a crucial role in internal investigations, particularly in the first stages that involve evidence retention and review (see Sections III.ii and V.ii).

II YEAR IN REVIEW

i Litigation

As mentioned in Section I, the CPC entered into force in 2016 and, along with making certain processes more efficient, introduced the following important changes, among others:

a encouragement of parties' active participation in conducting legal proceedings;
b promotion of in- and out-of-court mediation as an effective way of dispute resolution; and
c greater predictability of higher court decisions (including the Supreme Court).

The CPC also introduced other changes that may imply recognition of the discovery procedure in Brazilian law or, at the very least, a reinforcement of practices related to it.

The first change is the provision of a procedural agreement, which allows parties to create or stipulate the rules of the procedure, within the limits of public policy, and allows parties to control the case alongside the judge. This innovation, which has been inspired by arbitration practices, means that procedures could be structured according to the needs and peculiarities of each case, and, further, that parties can stipulate discovery rules. However, it has not been fully explored by parties to date and it has generally only been used for simpler purposes, such as electronic subpoenas and changing the order of the procedural steps. As mentioned, one reason for this is that parties require the judge's approval, which may not be easy to obtain.

The CPC does contain certain timid provisions that resemble the discovery procedure. The first is 'early evidence', which was enhanced to be an effective mechanism to resolve emerging disputes and prevent the submission of a complaint before the court. When submitting the early evidence, a party will ask the judge to consider the evidence in light of another conflict arising. The judge's decision may not only contribute to a better understanding of the current conflict, but may also help the parties to reach a settlement. Early evidence can be any type of evidence, such as the hearing of witnesses, accounting or engineering evidence, and the request for disclosure of specific documents.

ii Internal investigations

The most high-profile corporate investigation under way involves Brazil's state-run oil company Petrobras. This investigation, known as Operation Car Wash, began in March 2014 and has exposed endemic political corruption, and prompted a number of spin-off investigations. Law enforcement bodies are now emphasising that allegations of wrongdoing must be addressed internally. Authorities and regulators have also been welcoming the assistance of internal investigators to strengthen leniency agreements, considering factors such as a corporation's willingness to expose employees' or management's wrongdoing. In January 2018, Law No. 13,608 was published, which authorises telephone hotlines and provides rewards for whistle-blowers who offer information that prevents, represses or determines crimes or administrative offences. However, the Law is not being effectively enforced owing to a lack of clear regulations.

New legislation establishing regulations on e-discovery and internal investigations is not anticipated. However, since 2014 there have been certain ongoing issues, one of which is timing. The authorities generally conduct their own investigations to gather the necessary evidence to ensure convictions, although through leniency agreements and plea deals, legal entities and individuals, seeking to cooperate and obtain benefits, may

voluntarily present evidence of wrongdoing and illicit acts under Law No. 12, 846 of 2013 (the Clean Company Act).[2] Article 16 of the Clean Company Act establishes that leniency agreements must result in the identification of those involved in the wrongdoing, or in the rapid gathering of information or documents that prove the wrongful act under investigation.

Another issue relates to understanding the nature of ESI available for investigation. The use of instant messaging has vastly increased in the past few years and, in Brazil, most employees and businesses communicate with each other and with clients via WhatsApp.[3] This adds a layer of complexity to the collection and preservation of user data, but if it fails to be considered in investigations, critical evidence will be missed.

III CONTROL AND PRESERVATION

i Litigation

As there is no legal procedure for discovery, the concept of control in the context of ESI is not applicable.

ii Internal investigations

Not all companies have invested in data storage plans or clear retention policies and controls. Therefore, investigators must seek to understand which ESI is relevant for the investigation and if it is available. If the information is stored on a company-owned device, it may be collected. The most common sources for collection are: mobile phones; emails (from desktops, on-site laptops, tablets and any other corporate devices); electronically stored written documents; instant messages; network systems that log calendars and events; backup tapes; cloud storage; SD cards, USB drives and external hard drives; shared directories; and restored deleted files.

Relying on good-faith efforts of employees to ensure preservation of relevant ESI has also been a challenge. It is not uncommon for investigators to find that deletion of key information occurred immediately before or during the data collection and preservation process. As mentioned in Section I.ii, rather than being preventative, notifying employees or issuing hold notices has resulted in the destruction of evidence. A well-maintained chain of custody can help to protect investigators and companies from being questioned by authorities if evidence has been destroyed.

Preservation is limited to the observance of employee privacy rights. The labour courts have decided that a company may monitor and retain information from corporate devices supplied by it. Considering that it is common for employees to use corporate devices for personal communications, it is recommended to have employees sign a policy or a consent form, which clearly states that the information available on corporate devices is subject to retention and review. Personal devices, even if used for business purposes, may not be accessed by internal investigators unless authorised by the user. In that respect, employers are advised to prohibit the use of personal devices for corporate matters (see Section VI).

2 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

3 According to the *Harvard Business Review*, 96 per cent of Brazilians with access to a smartphone use the app as their primary method of communication. https://hbr.org/2016/04/the-rise-of-whatsapp-in-brazil-is-about-more-than-just-messaging.

Challenges abound with respect to the review of ESI that is personal in nature but not explicitly covered by the law – for example, income tax declarations, bank statements, passwords and health information.

Despite the absence of rules and sanctions for failure to preserve documentation, investigators who do not thoroughly check servers, databases and archives for relevant documents may be held accountable for conducting the investigation in a reckless manner or engaging in deliberate fraud if the results of the probe are disclosed to authorities.

IV REQUESTS AND SCOPE

As there is no disclosure procedure, parties do not need to meet and confer in the context of disclosure of ESI.

The CPC provides that a party may request the disclosure of specific documents prior to the start of a lawsuit through the early evidence procedure (see Section II.i) or during the course of a lawsuit. The interested party will ask the court to order the other party or a third party to disclose a certain document that is in its possession.

One of the following three conditions must be met in order for a party to seek and obtain a judicial order for disclosure of specific documents: (1) the opposing party has a legal duty to share the document; (2) the opposing party claims that it has a document that supports its position but fails to submit it before the court; or (3) the document belongs to both parties as a result of its contents.

According to the CPC, a party may refuse to disclose a specific document for the following reasons:

a if the document is related to the private life of any individual in the party, or if disclosure might compromise the duty of confidentiality to an individual or a third party, and any relatives up to the third degree, and doing so presents a risk of criminal prosecution;

b if it would entail disclosing facts that it, by order of the state or for professional reasons, must keep confidential (e.g., a memorandum by a lawyer to his or her client); and

c if there are other serious reasons that, according to the court's discretion, justify the refusal.

If a party fails to justify its reasons for not disclosing the requested documents, the court may order inductive, coercive, mandatory or subrogative measures for the document to be presented in court. These measures may also be taken against third parties that refuse to disclose a document without justification. If these measures are not successful, the court may presume and legally consider, for the specific case, that the facts related to the documents that were not disclosed are true.

V REVIEW AND PRODUCTION

i Litigation

As there is no disclosure procedure, the use of advanced analytical tools (e.g., technology-assisted review or predictive coding) to facilitate analysis, review and production is not applicable.

ii Internal investigations

Reviewing ESI in the context of an internal investigation is challenging considering that the scopes of most investigations are broad and communications concerning wrongdoing are often unclear or coded. Analytical tools, predictive coding and search technologies are starting to become available, but are not commonly used. Investigators should construct their keywords and queries with aim of narrowing down the scope of documents to identify evidence. The investigative team should also consider specific 'free searches' within the metadata files, such as 'to', 'from' and 'subject'. Search parameters, data ranges and various search methodologies should be explored.

Moreover, imprecise or careless search terms may be considered as an attempt to carry out evasive investigations that focus on irrelevant results.

The time frames for e-discovery and review of ESI depend on the number of documents available for analysis. To date, internal investigations in connection with Operation Car Wash have usually lasted from six to nine months. Investigations related to wrongdoing other than corruption are usually completed within three months.

VI PRIVACY ISSUES

The CPC grants the possibility of disclosure of specific documents, provided that the party requesting disclosure produces evidence of its right to do so. However, the opposing party may argue that the document is confidential and may refuse to present it before court, as provided by Article 404, IV, of the CPC. See Section IV.

On 14 August 2018, the then President Michel Temer enacted the Brazilian General Data Protection Law (LGPD), Law No. 13,709 of 2018, which is very similar to the European Union General Data Protection Regulation. Following the 18 months of *vacatio legis*, the LGPD will become effective in February 2020.

As a result of the LGPD provisions concerning the collection, use, processing and storage of personal data, companies will have to revisit their policies to ensure that employees are aware that information contained in corporate devices is subject to internal monitoring. Consequently, the use of personal devices for the exchange of corporate emails or business communications should be prohibited.

As a result, information governance programmes will have to be revisited in view of the LGPD; a well-maintained programme and a retention policy are key tools for companies to ensure preservation of ESI.

VII OUTLOOK AND CONCLUSIONS

Considering the corruption investigations of the past few years, legislative developments regarding e-discovery may be introduced, though it is unlikely that the legal framework will change substantially. Brazil is witnessing a shift in corporate culture concerning corruption and bribery schemes. As corporations' anti-corruption efforts and monitoring of compliance programmes are expected to become routine practice, new guidelines, protocols and tools related to e-discovery and internal investigations are likely to be created. It remains an open question as to how and when these will be implemented.

Chapter 5

CANADA

Anne Glover[1]

I OVERVIEW

The Canadian court system has two main arms: provincial and territorial, and federal.[2] There are 10 provinces and three territories.[3] The court system is roughly the same across Canada, except in Nunavut (one of the territories). Each province has three levels of courts – a provincial or territorial court, a superior court and an appellate court. Nunavut has a single trial court. The courts apply common law principles, except in the province of Quebec, where the courts apply the Quebec Civil Code.[4] The federal arm consists of the Federal Court (which specialises in areas such as intellectual property, maritime law and federal provincial disputes), the Tax Court and the Federal Court of Appeal.[5] The Supreme Court of Canada is Canada's final court of appeal.[6]

In all provinces but Quebec, the discovery process starts once pleadings are closed. At this point, the parties are required to list all documents that are relevant to the proceeding that are or have been in the parties' possession, power or control, even if the documents will not be used at trial. The test for relevance is broad, if a document contains any information that touches on the issues in the case, it is relevant.[7] Once the lists are provided, the other parties can serve a notice to inspect the documents listed. If the other parties want a copy of the documents listed, they are entitled to obtain copies at their own expense. In practice, however, it is now more common for parties to exchange copies of all documents electronically.

---

1 Anne Glover is a partner at Blake, Cassels & Graydon LLP. The author would like to thank the following contributors to this chapter: Melissa Feriozzo, Rebecca Kim, Alison Henderson and Anne Laverty.

2 See Canada's Court System, Can. Jud. Council, https://www.cjc-ccm.gc.ca/english/resource_en.asp?selMenu=resource_courtsystem_en.asp#ptc (last visited Aug. 24, 2018) [https://perma.cc/7G9V-Q738] (describing the jurisdiction of the provincial/territorial courts and the federal court).

3 Provinces and Territories, Gov't Can. (July 25, 2018), https://www.canada.ca/en/intergovernmental-affairs/services/provinces-territories.html (last visited Aug. 24, 2018) [https://perma.cc/4SPX-A58B].

4 See Peter Doody et al., Court System of Canada, Historica Can. https://www.thecanadianencyclopedia.ca/en/article/courts-of-law/ (last updated Feb. 28, 2018) [https://perma.cc/3KDH-2ZY7] (stating that the Civil Code is the relevant source of law in Quebec).

5 See Can. Jud. Council, *supra*, note 2; *supra* note 4 (stating that the federal court has jurisdiction over disputes with the federal government, maritime issues and intellectual property claims).

6 Doody et al., *supra* note 4.

7 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 30.02 (Can.) (stating that all relevant documents are within the scope of discovery); see also, e.g., Court Rules Act, B.C. Reg. 168/2009 Rule 7–1 (Can.); Court of Queen's Bench Rules, Man. Reg. 553/88 Rule 30.02(1) (Can.); N.B. Rules of Court, Rule 31.02 (Can.).

The province of Quebec is governed by civil law. This stems from when Quebec was founded by France in 1663 as 'New France'. The application of civil law continued even once France ceded sovereignty over Quebec to Britain. Document discovery in Quebec is set out in the Quebec Code of Civil Procedure (the Code) and differs from the rules applicable in the other provinces of Canada (which follow common law). One notable difference between the two systems is that, in Quebec, there is no general duty to produce or list all relevant documents that have been in a party's possession, power or control, especially if they are not intended to be used at trial.[8] For many years in Quebec, parties only had to produce documents they intended to rely on. In addition, parties had to write each other request letters setting out what documents they wanted disclosed.

In 2016, revisions were made to the Code in several areas, including document discovery. The Code now emphasises the obligation to preserve evidence,[9] cooperate and communicate diligently. In terms of resource allocation, the Code is still more restrictive than common law, directing all parties to limit the discovery to only 'what is necessary to resolve the dispute'.[10] The Code now provides detailed mechanisms for gathering and collecting evidence before judicial proceedings take place.[11]

II YEAR IN REVIEW

The following themes have been prevalent in Canadian case law over the past few years: proportionality; the use of technology in the discovery process; and the need for parties to cooperate in the discovery process.

i Proportionality

In *6Points Food Services Ltd v. Carl's Jr Restaurants LLC et al*,[12] the plaintiff produced 24,000 documents. The defendants brought a motion asking the court to order the plaintiff to produce fewer documents, complaining that the plaintiff was attempting to 'bludgeon' them into settlement by its massive and unorganised production.[13] The defendants did a random sampling of the plaintiff's production and found irrelevant documents, including dental benefits and plumbing receipts. The plaintiff had also produced documents from over 1,000 different authors. The defendants wanted the court to order the plaintiff to reduce the number of relevant documents. The court, while recognising the principle of proportionality and its aim at reducing unruly and costly discovery, refused to do this, saying that it would 'land the parties back before me and unduly intrudes on 6Points [the plaintiff] disclosure decisions'.[14] However, the court did find that the plaintiff did not do the work required to streamline its production and ordered it to categorise or index its production to make it more meaningful and manageable.

8 Bradley J. Freedman, Discovery of Electronic Records Under Canadian Law – A Practical Guide, 18 *Intell. Prop. J.* 59, 63–64 (2004).

9 Code of Civil Procedure, C.Q.L.R., c C–25.01, s 20 (Can.).

10 ibid., at a 19 (Can.).

11 ibid., at a 253–57 (Can.).

12 *6Points Food Services Ltd. v. Carl's Jr. Restaurants LLC et al.*, 2018 ONSC 7469 at para 1.

13 ibid.

14 ibid., at para 27.

ii Technology

In Ontario, the Superior Court of Justice has affirmed that parties should consider the use of appropriate technology when formulating a discovery plan to reduce costs and time,[15] and has implicitly endorsed the use of predictive coding.[16] At the federal level, the Canadian Competition Bureau has encouraged the use of technology in discovery to assist in 'document-heavy cases where they are as or more effective than the usual method of document collection and review'.[17]

iii Cooperation

In *Thompson v. Arcadia Labs Inc*,[18] the parties failed to agree on a protocol for the production and exchange of electronic documents. The court agreed with the defendant that there should have been far more engagement between counsel about the form and method of production of documents that were not in dispute. The court clearly stated that a party cannot use volume or the arduous nature of making proper and complete discovery to avoid fulfilling discovery obligations: 'Each party is obligated in good faith to produce the documents that tend to prove or disprove material allegations in dispute whether it helps or hurts the producing party. Jurisprudence establishes that a party cannot simply produce a banker's box or filing cabinet of paper and invite the other party to look through it. This is no different in the electronic world. Documents must be identified with precision.'[19] The court ordered counsel to 'meet, confirm and co-operate to eliminate all technical issues which are impeding the efficient exchange of documents. They should try resolutely to eliminate, narrow or focus any disagreement regarding scope.'[20]

In *Koolatron v. Synergex*,[21] the plaintiff brought a motion asking for, inter alia, production of additional documents to satisfy undertakings made during examinations.[22] The defendants argued that the cost to produce the additional documents was disproportionate to the modest amount at stake.[23] Justice Price stated the parties' failure to create a discovery plan, especially with respect to additional documents, impeded his ability to decide the issues.[24] In his order, Justice Price dismissed the plaintiff's production request without prejudice to the plaintiff's right to bring another motion once the discovery plan was in place. Moreover, the defendants were ordered to cooperate with the plaintiff in forming a discovery plan, including detailing where the additional documents were located and estimating the costs of production.[25] Although the plaintiff was largely successful in the motion (and thus would typically be entitled to costs), no costs were awarded because the failure to establish a discovery plan 'contributed to the necessity of the motion'.[26]

15 *Fincantieri Marine Systems North America Inc. v. Anmar Energy Ltd.*, 2015 ONSC 219 at para 27.
16 *Bennett v. Bennett Environmental Inc.*, 2016 ONSC 503 at paras 41 to 44.
17 *The Commissioner of Competition v. Live Nation Entertainment, Inc. et al.*, 2018 Comp Trib 17 at para 15.
18 *Thompson v. Arcadia Labs Inc.*, 2016 ONSC 3745 at para 11.
19 ibid., at para 19.
20 ibid., at para 24.
21 *Koolatron v. Synergex*, 2017 ONSC 4245 at para 57.
22 ibid., at para 18.
23 ibid., at para 19.
24 ibid., at para 63.
25 ibid., at para 81.
26 ibid., at para 79.

III CONTROL AND PRESERVATION

In most provinces in Canada,[27] parties to a lawsuit must disclose all documents in their possession, control or power relating to any matter at issue in the action.[28] Throughout Canadian jurisdictions 'document' is broadly defined, and includes data and information stored electronically.[29] A document is deemed to be in a party's possession, power or control if that party is entitled to obtain the original document or a copy of it and the party seeking disclosure of the document is not entitled to do the same.[30]

The rules of court in some jurisdictions give specific guidance regarding the control of electronically stored information (ESI). In the province of Nova Scotia, ESI is considered to be in the control of a party if it is 'in a database accessed by the party to the exclusion of another party' or if the party controls the ESI even though they 'can access [it] only through a custodian who is not an employee or an officer of the party'.[31] These kinds of ESI must be disclosed and produced as well as ESI contained on a computer or a storage medium actually or formerly possessed by a party.[32]

The province of Saskatchewan similarly delineates how ESI must be disclosed.[33] The parties should typically produce electronic documents kept in their 'active data and any other information that was stored in a manner than anticipated future business use, and that still permits efficient searching and retrieval'.[34] Generally, the parties are not obligated to produce documents that have been corrupted or deleted, as long as no agreement or order has been made to the contrary.[35]

The preservation duty for ESI arises as soon as litigation is reasonably anticipated, though when that exactly occurs depends on the facts of each case.[36] The dynamic nature of many types of ESI, as well as the ease with which ESI may be overwritten, hidden, altered or completely deleted, highlights the importance for early meetings and agreement on

27 This does not include the province of Quebec.

28 Rule 30.02, Ontario Rules of Civil Procedure, R.R.O 1990, Reg 194; Rule 7-1, [British Columbia] Supreme Court Civil Rules, BC Reg 168/2009; Rule 30.02, [Manitoba] Court of Queen's Bench Rules, Man Reg 553/88; Rule 31.02, [New Brunswick] Rules of Court of New Brunswick, NB Reg 82-73; Rule 219, [Northwest Territories] Rules of the Supreme Court of the Northwest Territories, NWT Reg R-010-96.

29 *Reichmann v. Toronto Life Publishing Co.* (1988), 30 C.P.C. (2d) 280 (Ont. H.C.) (where the definition of 'document' included a computer disc used to store information; if information could be derived from possession of the disc that was not provided by the product of the disc, there might be a gap in the operation of the rule); Rule 30.01(1), [Ontario] Rules of Civil Procedure, R.R.O 1990, Reg 194; [Manitoba] Rule 30.01, Court of Queen's Bench Rules, Man Reg 553/88; Rule 31.01, [New Brunswick] Rules of Court of New Brunswick, NB Reg 82-73; Rule 218, [Northwest Territories] Rules of the Supreme Court of the Northwest Territories, NWT Reg R-010-96.

30 *Ivey v. Canada Trust Co.* (1962), [1962] O.W.N. 62 (Ont. Master) (a party is not required to produce documents merely loaned to it); *Continental Can Co. v. Bank of Montreal* (1974), 3 O.R. (2d) 167 (Ont. H.C.) (the court may refuse to compel a party to produce a document where that party has no legal right to deal with it; the party will be required, however, to disclose the document's existence).

31 Rules 14.13 and 16.03, Nova Scotia Civil Procedure Rules, Royal Gaz Nov. 19, 2008 <http://canlii.ca/t/52m88>.

32 ibid.

33 Rule 5.7 of the Saskatchewan Queen's Bench Rules refers to the Civil Practice Directive No. 1 E-Discovery Guidelines 1 CIV-PD No. 1 regarding the use of electronic documents.

34 Civil Practice Directive No. 1 E-Discovery Guidelines 1 CIV-PD No. 1 at p. 47.

35 ibid.

36 *Corbett v. Corbett*, 2011 ONSC 1602 at para 27.

preservation among parties. Otherwise, parties may have differing expectations of what type of ESI to preserve, especially where one party has a very specific request, such as internet browsing history on a personal computer.[37]

Once it is determined that a preservation right has been triggered, a legal hold should be put in place. It is also a best practice (although not required) to serve the opposing party with a legal hold providing clear instructions detailing the kinds of information that should be preserved.[38] In exceptional cases, parties may obtain an *Anton Piller* order to immediately freeze or hand over ESI, if the evidence is essential to the other party and there is a genuine risk that it will be destroyed. A court may infer such a risk based on other dishonest conduct of a defendant as well as the ease with which certain types of evidence may be removed or disposed of, which may be particularly likely with ESI.[39]

Where a party has improperly failed to preserve relevant ESI, courts may respond pursuant to their rules regarding abuse of process or contempt. Courts have broad discretion to remedy such failures through awards of costs; refusing to allow a party to introduce evidence that was not properly preserved without leave; requiring a party who has destroyed or lost relevant evidence to bear the cost of recovering the evidence; or in cases of intentional destruction, by allowing an adverse inference that the destroyed document would have not been helpful to the destroying party's case.

The availability of a separate tort of spoliation in Canada remains uncertain. If this tort did exist, the courts have stated that there would be a high threshold for the finding of spoliation. It would require intentional destruction of relevant evidence for the purpose of influencing the outcome of the litigation.[40]

IV REQUESTS AND SCOPE

As noted in Section I, the document discovery process commences once pleadings are closed. At this point, the parties are required to list all documents that are relevant to the proceeding that are or have been in their possession, power or control, even if the documents will not be used at trial.

The test for relevance in most provinces is very broad: if a document contains any information that touches on the issues in the case, it is relevant. In *Imperial Oil v. Jacques*,[41] the Supreme Court of Canada recognised that the concept of relevance is generally interpreted broadly at the exploratory stages of an action. Saskatchewan courts have affirmed that 'relevance is broader on discovery than at trial, and greater latitude is permitted at this stage of the proceedings than later'.[42]

Some provinces in Canada are putting in place rules that require the parties to meet and confer before document discovery takes place. In Ontario, the parties are required to enter

37 *Catalyst Capital Group Inc. v. Moyse*, 2016 ONSC 5271.

38 ibid., at 25.

39 ibid., at 28; *Noreast Electronics Co. Ltd. v. Danis*, 2018 ONSC 879.

40 *Catalyst Capital Group Inc. v. Moyse*, 2016 ONSC 5271; 2018 ONCA 283.

41 *Imperial Oil v. Jacques*, 2014 SCC 66.

42 *Cominco Ltd. v. Phillips Cables Ltd.* [1987] 3 W.W.R. 562 at para 11; the broad relevance test has been affirmed in cases such as *Gulka Enterprises Ltd v. Bayer Cropscience Inc.* 2009 SKQB 101 at para 4, 101239408 *Saskatchewan Ltd. v. S-5 Holdings Ltd.* 2016 SKQB 144 at paras 17 to 19 and *Smith v. Dawgs Canada Distribution Ltd.* 2012 SKQB 305 at paras 2 to 5.

into a discovery agreement before any discovery is commenced.[43] The discovery agreement is to contain the following: the scope of document discovery; dates for the service of the list of documents; information on timing, costs (including who will pay for discovery) and how documents are to be produced; the names of people intended to be produced for oral discovery; and any other information intended to result in the expeditious and cost-effective completion of the discovery process.[44]

In British Columbia, a case-planning conference can either be requested by a party or administered by the court.[45] If a case planning conference is requested or ordered, the parties must file case plan proposals with respect to the following steps: (1) discovery of records; (2) examinations for discovery; (3) dispute resolution processes; (4) expert witnesses; (5) list of witnesses; and (6) type of trial, estimated trial length and preferred trial dates.[46] At a case-planning conference, the judge or master may make an order addressing any of these factors.[47]

Many of the provinces in Canada have also adopted the Sedona Canada Principles Addressing Electronic Discovery. In Ontario, the Rules of Civil Procedure state that in preparing the discovery plan, 'the parties shall consult and have regard' to the Sedona Canada Principles.[48] One of those principles is proportionality. That principle has been adopted into the Ontario Rules in Rule 29.1, which is entitled 'Proportionality in Discovery'. Under this Rule, in determining if a party must produce a document, the court is to consider the following factors:

a whether the time required to produce the document would be unreasonable;
b whether the expense would be unreasonable;
c whether producing the document would cause the party undue prejudice;
d whether requiring the party to produce the document would interfere with the orderly progress of the action;
e whether the document is readily available to the party requesting it from another source; and
f whether such an order would result in the party having to produce an excessive volume of documents.[49]

In Saskatchewan, Rule 5.7 of the Queen's Bench Rules directs the reader to the Civil Practice Directive on E-Discovery Guidelines for the use of electronic documents.[50] The Practice Directive states, 'parties in actions which involve e-discovery should consult and have regard' to the Sedona Canada Principles.[51] This Practice Directive emphasises the importance of proportionality and elaborates on the required disclosure of electronic documents that have direct relevance.[52]

43 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 29.1.
44 ibid.
45 British Columbia Supreme Court Civil Rules, B. C. Reg. 168/2009, Rule 5.1.
46 ibid.
47 British Columbia Supreme Court Civil Rules, B. C. Reg. 168/2009, Rule 5.3.
48 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 29.1.03(4).
49 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 29.2.03(1).
50 Saskatchewan Queen's Bench Rules, Rule 5.7.
51 Saskatchewan Civil Practice Directive No. 1 E-Discovery Guidelines 1 CIV-PD No. 1 at p. 46.
52 ibid., at pp. 46–47.

Although the British Columbia Supreme Court Civil Rules do not refer directly to the Sedona Canada Principles, Rule 1.3 includes proportionality as an essential element to achieving its objective of ensuring a 'just, speedy and inexpensive determination of a proceeding on its merits'.[53]

In *Palmerston Grain, A Partnership et al v. Royal Bank of Canada*,[54] two motions regarding electronic discovery (e-discovery) were before the court. One issue to be decided was whether there was a discovery plan in place that satisfied the parties' obligations under the Ontario Rules of Civil Procedure. The court reviewed the relevant Rules and the Sedona Canada Principles. The court stated that 'parties are required to comply with the Sedona Principles and failing to do so is a breach of the rules.'[55] The court held that the discovery plan did not constitute a discovery plan as it did not contain the content required by the Rules.

In *City of Ottawa v. Suncor Energy Inc.*,[56] a motion regarding electronic discovery was before the court. A diesel fuel spill occurred at an articulated bus garage, which was located on property owned by the city of Ottawa. The city claimed damages against Suncor, the supplier of the diesel fuel, and Transport Jacques Auger Inc., which was responsible for delivering the fuel. Suncor and Auger started third-party proceedings against several companies involved in building the garage, including EllisDon Corporation. The parties involved did not establish a discovery plan before starting examinations for discovery.[57] During the examinations for discovery, EllisDon gave undertakings to provide information relevant to the EdgeBuilder, the Project System and the Fuel Management System.[58] Although EllisDon produced its database on a portable drive, Suncor and Auger experienced difficulties when accessing these records, particularly owing to the number of irrelevant records that had been included. Suncor and Auger brought a motion for EllisDon to answer the undertakings by taking further action to produce documents in a more accessible manner. The court held that EllisDon must answer the undertakings by removing any irrelevant documents from the portable drive, adding a unique identifier to each document on the portable drive and meeting to discuss a discovery plan.[59] The court referred to the Sedona Canada Principles and the requirement to develop a discovery plan, stating that 'participation in discovery planning is one element of counsel's duty as an officer of the court. In fulfilling that aspect of their duty, counsel are required to apply the principles of proportionality while seeking maximum procedural efficiency.'[60] Furthermore, the court stated that the 'party producing the documents must identify them with precision'.[61]

V REVIEW AND PRODUCTION

As noted above, the law in Canada is that parties must review and produce documents with precision.[62] In most provinces, parties are also required to provide a privilege log, although

53 British Columbia Supreme Court Civil Rules, B. C. Reg. 168/2009, Rule 1.3(2).
54 *Palmerston Grain, A Partnership et al v. Royal Bank of Canada*, 2014 ONSC 5134.
55 2014 ONSC 5134 at para 45.
56 *City of Ottawa v. Suncor Energy Inc.*, 2019 ONSC 1340.
57 2019 ONSC 1340 at para 6.
58 ibid., at para 17.
59 ibid., at para 41.
60 ibid., at para 29.
61 ibid., at para 31.
62 ibid., at para 31.

in practice this does not happen in each case. The timing for production of documents is governed by the Rules of Court in each province. Despite these rules, parties often negotiate the timing for the production of documents between themselves.[63]

If a party believes that potentially relevant documents have not been disclosed or that privilege has been improperly asserted over relevant documents, the party may demand that the opposing party produce the documents or bring a motion to the court regarding same.[64] Where the court determines that the affidavit of documents (AOD) is not complete or a claim of privilege has been improperly made, the court may order the party to provide a more extensive AOD, order cross-examination on the AOD or assess the documents to determine whether or not they must be produced. [65]

The court may impose sanctions against a party for failing to comply with the rules of court regarding the disclosure or production of relevant documents. In the province of Ontario, if a party fails to disclose a document in its AOD, there is a presumption that the non-disclosing party may not use the document at trial.[66] If the document is favourable to the non-disclosing party, then the party may only use the document with leave of the trial judge.[67] If the document is unfavourable, then the court will have discretion to make it available to the

63 In Alberta, the plaintiff must provide the affidavit of records to the opposing party within three months of being served with the statement of defence, while the defendant must provide the affidavit of records within two months of receiving the plaintiff's affidavit of records (Alberta Rules of Court, Rule 5.5). In Saskatchewan, the plaintiff must serve the AOD within 30 days of receiving the statement of defence, whereas the defendant must serve the AOD within 30 days subsequent to this (Saskatchewan Queen's Bench Rules, Rule 5.5). The Nova Scotia Civil Procedure Rules specifically address the disclosure of electronic information, delineating that an 'affidavit disclosing electronic information' and all relevant electronic information that is not privileged must be disclosed within 45 days of the close of pleadings (Nova Scotia Civil Procedure Rules, Rule 16.07 and 16.09). In the province of British Columbia, all parties must produce a list of documents within 35 days of the close of pleadings (British Columbia Supreme Court Civil Rules, Rule 7.1(1)). In Manitoba, Newfoundland and Prince Edward Island, the parties to an action must similarly produce an AOD within 10 days of the close of pleadings (Manitoba Court of Queen's Bench Rules, Rule 30.03(1); Newfoundland Rules of the Supreme Court, Rule 32.01; Prince Edward Island Supreme Court Rules of Civil Procedure, Rule 30.03). In New Brunswick, a party may serve a notice requiring an AOD, upon receipt of which the party is required to provide an AOD within 30 days (New Brunswick Rules of Court, Rule 31.03).

64 Alberta Rules of Civil Procedure, Rule 30.06; British Columbia Supreme Court Civil Rules, Rule 7.1(10)-(17); Manitoba Court of Queen's Bench Rules, Rule 30.04; New Brunswick Rules of Court, Rule 31.04; Newfoundland Rules of the Supreme Court, Rule 32.06; Nova Scotia Civil Procedure Rules, Rule 14.09; Ontario Rules of Civil Procedure, Rule 30.04; Prince Edward Island Supreme Court Rules of Civil Procedure, Rule 30.04; Saskatchewan Queen's Bench Rules, Rule 5.11-5.12(1).

65 Alberta Rules of Civil Procedure, Rule 30.06; British Columbia Supreme Court Civil Rules, Rule 7.1(14); Manitoba Court of Queen's Bench Rules, Rule 30.06; New Brunswick Rules of Court, Rule 31.06; Newfoundland Rules of the Supreme Court, Rule 32.07; Nova Scotia Civil Procedure Rules, Rules 14.12 and 16.14; Ontario Rules of Civil Procedure, Rule 30.06; Prince Edward Island Supreme Court Rules of Civil Procedure, Rule 30.06; Saskatchewan Queen's Bench Rules, Rule 5.12.

66 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 30.08(1)(a).

67 ibid.

non-disclosing party 'as is just'.[68] In general, courts will admit undisclosed documents, albeit with costs to the non-disclosing party and in some instances an adjournment.[69] Advertent concealment of relevant documents may lead to significant costs sanctions.[70]

The provinces of British Columbia, Manitoba, New Brunswick and Prince Edward Island have similar rules regarding the consequences of failure to comply. If a party fails to disclose a relevant document in its AOD, the rules of these provinces prescribe that the non-disclosing party may not use the document at trial unless the court orders otherwise.[71] In Newfoundland and Saskatchewan, the court may go so far as to order that the defence be dismissed and judgment entered accordingly, or to dismiss the proceedings entirely.[72]

It is a well-established rule in Canada that parties cannot use documents received through the discovery process for a collateral or ulterior purpose.[73] According to the Supreme Court of Canada, remedies for breach of this rule may include a stay or dismissal of the proceeding, striking a defence or even contempt of court proceedings.[74]

There is a small but growing number of cases that discuss the use of advanced analytical tools in e-discovery in Canada. In the Ontario case of *L'Abbé v. Allen-Vanguard*,[75] the court set out some general principles when conducting discoveries that involve vast numbers of documents, particularly ESI. The court emphasised the need to harness technology and referenced predictive coding and auditing procedures as e-discovery solutions.[76] In *Bennett v. Bennett Environmental Inc*,[77] the court tacitly approved the use of predictive coding. The use of advanced analytics received its most explicit endorsement in the recent case of *The Commissioner of Competition v. Live Nation Entertainment, Inc et al*.[78] This was a Competition Tribunal matter involving allegations of deceptive marketing practices.[79] In their affidavits of documents, the respondents declared that in conducting searches for relevant documents using technology-assisted review (TAR), they had found no relevant documents in their possession, control or power.[80] The Commissioner of Competition objected to the affidavits of documents on the basis that the search for documents was inadequate.[81] The Competition

68 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 30.08(1)(b).

69 ibid., Rule 53.08(1)-(2).

70 See Todd Archibald, James Morton and Sam Sasso, *Discovery in Canadian Common Law* (Toronto: LexisNexis Canada Inc., 2017) at 67.

71 British Columbia Supreme Court Civil Rules, Rule 7.1(21); Manitoba Court of Queen's Bench Rules, Rule 30.08; New Brunswick Rules of Court, Rule 31.08; Prince Edward Island Supreme Court Rules of Civil Procedure, Rule 30.08.

72 Newfoundland and Labrador Rules of the Supreme Court, Rule 32.10; Saskatchewan Queen's Bench Rules, Rule 5.14(2); Saskatchewan Queen's Bench Rules, Rule 5.14(2).

73 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 30.1, codifying the Common Law 'deemed or implied undertaking' rule. See Archibald et al., *supra* note 70, at 162–165.

74 *Juman v. Doucette*, 2008 SCC 8 at para 23.

75 *L'Abbé v. Allen-Vanguard*, 2011 ONSC 7575.

76 ibid., at paras 21 and 23.

77 *Bennett v. Bennett Environmental Inc.*, 2016 ONSC 503.

78 *The Commissioner of Competition v. Live Nation Entertainment, Inc. et al*, 2018 Comp Trib 17.

79 ibid., at para 2. The Competition Commissioner alleged that the respondents promoted the sale of tickets to the public at prices that are not in fact attainable.

80 ibid., at para 5.

81 The Commissioner had previously obtained documents from a respondent that did not end up in the applicable affidavits of documents, including documents relating to the Respondents' marketing practices, consumer behaviour, and impact of the respondents' advertising (ibid., at para 6).

Tribunal had no objections to the use of predictive coding; the problem related to how TAR was used in this instance.[82] The Tribunal went on to explicitly approve the use of TAR: 'The Tribunal encourages the use of modern tools to assist in these document-heavy cases where they are as or more effective and efficient than the usual method of document collection and review.'[83]

The general rule in Canada is that the party in possession or control of the documents is to produce the documents at its expense. The courts have discretion to depart from this rule if fairness and justice so require, or if its application would financially prevent a party from presenting its case in the action.[84] When a case is over, the court has the discretion to award costs. There is a loser-pays cost system for most types of cases (but not for class actions in some provinces). In this type of system, the losing party may be ordered to pay some or all of the winning party's legal costs and disbursements (including lawyer's fees). The basic rule is that costs on a partial indemnity scale follow the event. 'Partial indemnity' means that the successful party does not recoup all its costs but a portion of them.[85] In Ontario, for example, a successful party often recovers 25 to 35 per cent of the actual costs incurred. These costs will include the costs of document discovery.[86] The court has discretion to depart from this normal rule, however, and order 'substantial indemnity' costs, which is meant to more closely match the costs actually incurred by the successful party.[87] Substantial indemnity orders are rare and generally only ordered if the unsuccessful party has engaged in misconduct or has acted in oppressive or vexatious ways.

As to the actual production of documents, the Sedona Canada Principles Addressing Electronic Discovery state that 'whenever possible, the production of ESI should be made in searchable electronic format.'[88]

VI PRIVACY ISSUES

Privacy in the private sector is subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs how private sector organisations handle personal information.[89] The provinces of Alberta, British Columbia and Quebec have enacted private sector privacy statutes which have been deemed 'substantially similar' to PIPEDA.

82 ibid., at para 14.

83 ibid., at para 15.

84 See *Veillette v. Piazza Family Tr.*, 2012 CanLII 5414, paras 18–20 (Can. Ont. Sup. Ct. J.) (asserting that the court has the discretion to depart from the general rule 'if its application would financially prevent a party from presenting their case in the action'); *Ho v. O'Young-Lui*, 2002 CanLII 6346, para 10 (Can. Ont. Sup. Ct. J.) ('[T]he court has a discretion to depart from [the general rule] where fairness and justice so require.').

85 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 1.03

86 A Comparative Discussion of Who Pays for Document Discovery in Australia, Canada, Guernsey (Channel Islands) and Singapore and its Effect on Access to Justice, *Vanderbilt Law Review*, Volume 71, Number 6, Nov. 2018, p. 2,158.

87 Ontario Rules of Civil Procedure, R.R.O. 1990, Reg. 194, Rule 1.03.

88 The Sedona Canada Principles Addressing Electronic Discovery, Second Edition, Nov. 2015, p. 53.

89 The public sector is governed by the Privacy Act and legislation in each province. There are also health sector privacy laws, which are not discussed in this chapter.

As such, PIPEDA does not apply to commercial organisations operating only within these jurisdictions other than federal works, undertakings or businesses (such as airlines, banks and telecommunications companies), which continue to be covered by PIPEDA.

Section 5(3) of PIPEDA sets out the 'appropriate purpose' principle of the legislation.[90] It states: 'An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider appropriate in the circumstances.'[91]

This term, 'that a reasonable person would consider appropriate in the circumstances', is an overarching requirement of Canadian privacy law. Lawyers and organisations are bound by this obligation in the discovery and disclosure of ESI.[92] As such, they must carefully assess the reasonableness and necessity of producing electronically stored personal information.[93] Courts will take privacy considerations into account when deciding whether to order the production of electronic devices containing sensitive personal information. As a general rule, courts are reluctant to grant discovery requests that are too broad or that involve non-relevant private information.[94] In the case of *Desgagne v. Yuen et al*, for example, the British Columbia Supreme Court cited privacy concerns in denying a request to produce a plaintiff's entire personal hard drive.[95]

Under PIPEDA's appropriate purpose principle, organisations are responsible for personal information in their custody or control, including personal information transferred to a third-party service provider for processing on the organisation's behalf. Personal information can be transferred to a service provider, without consent, where the transferring organisation uses contractual or other means to provide a comparable level of protection while the information is being processed by the service provider.[96,97]

PIPEDA does not distinguish between domestic and international transfers of data. If an organisation is transferring personal information to a service provider outside Canada, the Privacy Commissioner has stated that the organisation needs to make it clear to individuals that their information may be processed in a foreign country and may be accessible to law enforcement authorities of that jurisdiction.[98] This notice must be given in clear and understandable language and ideally when the information is collected.[99]

The coming into force of the European Union's General Data Protection Regulation (GDPR) on 28 May 2018 has potentially far-reaching consequences for the discovery of

90 Personal Information Protection and Electronic Documents Act, SC 2000, c 5, s 5(3).

91 ibid.

92 Office of the Privacy Commissioner of Canada, 'A Privacy Handbook for Lawyers: PIPEDA and Your Practice', online: OPC <https://www.priv.gc.ca/media/2012/gd_phl_201106_e.pdf> at 23 [OPC Privacy Handbook].

93 Susan Wortzman, ed, *E-Discovery in Canada*, 3rd ed (Toronto: LexisNexis Canada Inc., 2017) at 164.

94 See The Sedona Canada Principles Addressing Electronic Discovery, Second Edition, A Project of the Sedona Conference Working Group 7 (WG7), Nov. 2015 at 62.

95 *Desgagne v. Yuen et al*, 2006 BCSC 955 at para 40.

96 PIPEDA, Schedule 1, s 4.1.3 (Principle 1); see also OPC Privacy Handbook, *supra* note 92, at 23.

97 The Office of the Privacy Commissioner of Canada initiated a consultation in April 2019 entitled 'Consultation on Transborder Dataflows' whereby they propose to reverse this long held position and instead require consent for any transfer of personal information to a service provider for processing.

98 OPC Privacy Handbook, *supra* note 92 at 23.

99 Office of the Privacy Commissioner of Canada, 'Guidelines for Processing Personal Data Across Borders' (27 January 2009), online: Personal Information Transferred Across Borders <https://www.priv.gc.ca/en/privacy-topics/personal-information-transferred-across-borders/gl_dab_090127/>.

ESI in Canada as well.[100] Canadian-based organisations may be subject to the GDPR if they have an establishment in the European Union, process personal data in connection with the offering of goods or services to individuals in the European Union or monitor the behaviour of individuals in the European Union.[101]

VII OUTLOOK AND CONCLUSIONS

The law of e-discovery in Canada is growing and developing. The principles of proportionality and reasonableness will, hopefully, continue to be adopted by the courts. We also hope to see the courts continue to endorse the use of technology in the discovery process. This progress is essential given the proliferation of electronic documents in this digital age.

100 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1 [GDPR].

101 GDPR, article 3(2). The GDPR also applies if the data processing activities are related to monitoring the behaviour of individuals in the European Union.

Chapter 6

ENGLAND AND WALES

Afzalah Sarwar[1]

I OVERVIEW

i Rules of disclosure

The rules relating to disclosure in the context of English civil litigation are contained in the Civil Procedure Rules (CPR), which govern the practice and procedure for civil cases in England and Wales.[2] However, as England has a common law legal system, parties will also need to consider English case law to the extent that it is relevant to any issue that may arise.

Until 1 January 2019, the relevant rules were contained in Part 31 of the CPR. However, on this date, a new Disclosure Pilot Scheme (the Disclosure Pilot) was launched, creating a new mandatory framework for disclosure. The new rules are contained in Practice Direction 51U3 to Part 51 of the CPR, which includes the following appendices:

a Appendix 1: Definitions for the purpose of Section I;
b Appendix 2: Disclosure Review Document;
c Appendix 3: Certificate of Compliance; and
d Appendix 4: Disclosure Certificate.

The Disclosure Pilot will apply for two years from 1 January 2019 to existing and new proceedings in the business and property courts of England and Wales. The Disclosure Pilot will not disturb an order for disclosure made before 1 January 2019 or before the transfer of proceedings into a business and property court, unless that order is varied or set aside. The Disclosure Pilot will continue to apply after the end of the two-year period to any proceedings to which it applied at that point. The expectation, however, is that CPR Part 31 will be revised to reflect the new rules if the Disclosure Pilot is deemed a success, and consideration will be given as to whether its scope should be extended to other proceedings outside the business and property courts.[4] The courts that constitute the business and property courts include the Chancery Division of the High Court,[5] the Commercial Court[6] and the Technology and Construction Court.[7] Given that, between them, these courts handle the vast majority of

1 Afzalah Sarwar is of counsel at Morgan, Lewis & Bockius UK LLP.
2 Statutory Instrument 1998 No. 3132 (L.17).
3 https://www.justice.gov.uk/courts/procedure-rules/civil/rules/practice-direction-51u-disclosure-pilot-for-the-business-and-property-courts.
4 Disclosure Working Group Press Announcement, 31 July 2018: https://www.judiciary.uk/wp-content/uploads/2018/07/press-annoucement-disclosure-pilot-approved-by-cprc.pdf.
5 https://www.gov.uk/courts-tribunals/chancery-division-of-the-high-court.
6 https://www.gov.uk/courts-tribunals/commercial-court.
7 https://www.gov.uk/courts-tribunals/technology-and-construction-court.

high-value and complex commercial disputes, including those with a cross-border element,[8] the Disclosure Pilot is likely to have a huge impact on how businesses discharge their disclosure obligations over the next two years at least. This chapter focuses on the practice and procedure contained in the Disclosure Pilot, the background to which is addressed in Section II.

England adopts a 'cards on the table' approach to disclosure, whereby parties are required to disclose both helpful and harmful documents to the other side in advance of the final hearing on the merits of the case, at which point the judge will determine the issues in dispute. This early disclosure requirement, as well as the rules requiring parties to exchange witness statements of fact and expert reports ahead of the final hearing, enables the parties to assess the strengths and weaknesses of their respective cases at a relatively early stage, thereby potentially encouraging early settlement. It also seeks to avoid a 'trial by ambush'. This requirement for early disclosure was reinforced by the implementation of the Disclosure Pilot.

ii Stages of disclosure

There are two key stages for disclosure under the Disclosure Pilot.

Initial disclosure

Under the old regime, parties were generally required to give disclosure once the statements of case (such as the particulars of claim, defence and reply) had been filed and following the first case management conference at which the court would make an order setting out the procedural timetable for the proceedings, including the timeline for giving disclosure. However, under the new rules, at the same time as filing its statement of case, a party is required to provide the other party with a copy of the key documents on which it relies (expressly or otherwise) and the key documents that are necessary for the opposing party to understand the claim or defence it has to meet. This form of disclosure is known as initial disclosure and must be accompanied by an initial disclosure list, which lists the documents. The requirement for initial disclosure may, however, be dispensed with if (1) the parties agree, (2) the court has ordered that it is not required or (3) the initial disclosure would involve more than approximately 1,000 pages or 200 documents (or a higher, but reasonable, figure the parties have agreed), whichever is larger. The obligation to provide initial disclosure does not apply where a statement of case is to be served on a defendant out of the jurisdiction unless the defendant files an acknowledgment of service that does not contest jurisdiction.

Extended disclosure

After the initial disclosure stage, a party wishing to seek disclosure of documents in addition to, or as an alternative to, initial disclosure, must request extended disclosure. There is no presumption that a party is entitled to extended disclosure and there will be no extended disclosure without the court's approval. The court will usually deal with such a request at the first case management conference. However, before then, the court will expect the parties to have completed the disclosure review document (DRD), which is in Appendix 2 of the Disclosure Pilot. The first step will be for the parties to complete the list of issues for disclosure in Section 1A of the DRD. The Disclosure Pilot defines issues for disclosure to mean only those key issues in dispute that the parties consider will need to be determined by the court

8 See links in footnotes 4 to 6 for details as to types of cases that these courts handle.

with some reference to contemporaneous documents in order for there to be a fair resolution of the proceedings. It does not extend to every issue that is disputed in the statements of case by way of denial or non-admission.[9] The parties must also indicate in Section 1A of the DRD which disclosure model they propose for each issue for disclosure. The Disclosure Pilot refers to five disclosure models – Models A to E – for the purposes of extended disclosure,[10] which may be summarised as follows.

Model A: disclosure confined to known adverse documents

The court may order that the only disclosure required in relation to some or all of the issues for disclosure is of 'known adverse documents'.

A document is considered to be adverse if 'it or any information it contains contradicts or materially damages the disclosing party's contention or version of events on an issue in dispute, or supports the contention or version of events of an opposing party on an issue in dispute'.[11] The Disclosure Pilot introduced for the first time the concept of known adverse documents, which are 'documents (other than privileged documents) that a party is actually aware (without undertaking any further search for documents than it has already undertaken or caused to be undertaken) both (a) are or were previously within its control and (b) are adverse'.[12] For this purpose, a company or organisation is aware if any person with accountability or responsibility within the company or organisation for the events or the circumstances that are the subject of the case, or for the conduct of the proceedings, is aware. It will also be necessary to take reasonable steps to check the position with any person who was accountable or responsible but who has since left the company or organisation.[13]

Given that parties are already under a continuing obligation once proceedings have been commended to disclose known adverse documents, and regardless of any order for disclosure made,[14] Model A is effectively an order for no extended disclosure. This positive obligation to disclose known adverse documents does not exist under the CPR Part 31 regime.

Model B: limited disclosure

The court may order the parties to disclose (where and to the extent that they have not already done so by way of initial disclosure, and without limit as to quantity this time) those documents required for initial disclosure and, in addition, to disclose known adverse documents in accordance with their continuing duty.

A party giving Model B Disclosure is under no obligation to undertake a search for documents beyond any search already conducted for the purposes of obtaining advice on its claim or defence or preparing its statements of case. Where it does undertake a search, however, the continuing duty to disclose known adverse documents will apply.

9 Paragraph 7.3, Disclosure Pilot.
10 Paragraph 8, Disclosure Pilot.
11 Paragraph 2.7, Disclosure Pilot.
12 Paragraph 2.8, Disclosure Pilot.
13 Paragraph 2.9, Disclosure Pilot.
14 Paragraph 3.1(2), Disclosure Pilot.

Model C: request-led search-based disclosure

The court may order a party to give disclosure of particular documents or narrow classes of documents relating to a particular issue for disclosure by reference to requests set out in or to be set out in Section 1B of the DRD or otherwise defined by the court.

Any party proposing Model C extended disclosure must complete Section 1B of the DRD setting out the nature of the request.

A party giving Model C disclosure must still comply with the duty to disclose known adverse documents, which will include any arising from the search directed by the court.

Model D: narrow search-based disclosure, with or without narrative documents

Under Model D, a party will be required to disclose documents that are likely to support or adversely affect its claim or defence, or that of another party in relation to one or more of the issues for disclosure.

Each party is required to undertake a reasonable and proportionate search in relation to the issues for disclosure for which Model D disclosure has been ordered.

The order should specify whether a party giving Model D disclosure is to search for and disclose narrative documents. If the order does not specify this, narrative documents should not be disclosed. A narrative document is 'a document which is relevant only to the background or context of material facts or events, and not directly to the Issues for Disclosure'.

A party giving Model D disclosure must still comply with the duty to disclose known adverse documents, which will include any arising from the search directed by the court.

Model E: wide search-based disclosure

Under Model E, a party will be required to disclose documents that are likely to support or adversely affect its claim or defence, or that of another party in relation to one or more of the issues for disclosure or that may lead to a train of enquiry, which may then result in the identification of other documents for disclosure (because those other documents are likely to support or adversely affect the party's own claim or defence, or that of another party in relation to one or more of the issues for disclosure).

Model E is only to be ordered in an exceptional case.

Each party is required to undertake a reasonable and proportionate search in relation to the issues for disclosure for which Model E disclosure has been ordered. The scope of the search will be determined by the court using the information provided in the DRD and is likely to be broader than that ordered for Model D disclosure. Narrative documents must also be searched for and disclosed, unless the court otherwise orders.

A party giving Model E disclosure must still comply with the duty to disclose known adverse documents, which will include any arising from the search directed by the court.

Drafts of Section 2

Having agreed the list of issues for disclosure and exchanged proposals on models for extended disclosure, the parties are required to prepare and exchange drafts of Section 2 of the DRD, which comprises a questionnaire. As indicated in the DRD, the purpose of Section 2 is to provide the court with information about the data held by each party, including where and how the data is held; how the parties propose to process and search the data where a search-based disclosure model (Models C, D and E) is sought in relation to particular

issues for disclosure; and whether there are any points that the parties have not been able to agree through discussions and that they therefore need the court to determine at the case management conference. The parties are also required to provide an estimate of what they consider to be the likely costs of giving the disclosure proposed by them in the DRD, and the likely number of documents involved, so that a court may consider whether the proposals on disclosure are reasonable and proportionate.

Electronically stored information

As under the old regime, the definition of 'document' under the Disclosure Pilot extends to electronically stored information (ESI). The Disclosure Pilot provides that a document 'includes any record of any description containing information',[15] and confirms that emails and other electronic communications, such as text messages, webmail, social media, voicemail and audio or visual recordings, will fall within this definition, as will information stored on servers and backup systems and electronic information that has been deleted. It also extends to metadata and other embedded data that is not typically visible on screen or a printout.

Courts and parties were historically reluctant to utilise the available technology and analytic tools to manage ESI for the purposes of disclosure. This was likely owing to their lack of knowledge and experience in using e-disclosure technology coupled with a party's desire to ensure that its approach to disclosure was defensible and less likely to be challenged. However, in recent years, there has been a marked shift in the attitude of both the parties and courts to e-disclosure technology. The turning point was in 2016 when the English High Court delivered two key judgments. The judgment in *Pyrrho Investments Ltd v. MWB Property Ltd*[16] was the first reported decision expressly approving the use of predictive coding technology in circumstances where the parties consented to its use. However, it was later that year, in *Brown v. BCA Trading Ltd*,[17] that the English Court went one step further and delivered its landmark ruling permitting one party to use predictive coding technology for disclosure purposes, notwithstanding the other party's objection to its use. Moreover, the Disclosure Pilot expressly requires the parties to discuss and seek to agree matters that are relevant to those disclosure models that require searches to be carried out, such as the use of software or analytical tools, including technology-assisted review software and techniques. This is reflected in Section 2 of the DRD, which the parties are required to complete in advance of the first case management conference.

Filing the DRD

After the parties have completed Sections 1A, 1B and 2 of the DRD, a finalised, single, joint DRD must be filed by the claimant party no later than five days before the case management conference. The parties are then required to each file a signed certificate of compliance substantially in the form set out in Appendix 3 to the Disclosure Pilot in advance of the case management conference.

Where the court makes an order for extended disclosure, a party complies with that order by undertaking the following steps:[18] (1) service of a disclosure certificate substantially in the form set out in Appendix 4 to the Disclosure Pilot signed by the party giving disclosure,

15 Paragraph 2.2, Disclosure Pilot.

16 *Pyrrho Investments Ltd and another v. MWB Property Ltd and others* (2016) EWHC 256 (Ch).

17 *Brown v. BCA Trading Ltd* [2016] EWHC 1464 (Ch).

18 Paragraph 12.1, Disclosure Pilot.

to include a statement supported by a statement of truth signed by the party or an appropriate person at the party that all known adverse documents have been disclosed; (2) service of an extended disclosure list of documents (unless dispensed with, by agreement or order); and (3) production of the documents that are disclosed over which no claim is made to withhold production or if the party cannot produce a particular document, compliance with Paragraph 12.3 of the Disclosure Pilot.[19]

Costs

In English civil litigation, the general rule is that costs follow the event, which means that the unsuccessful party will be ordered to pay the costs of the successful party. However, the court retains a discretion to make a different order.[20] Paragraph 20 of the Disclosure Pilot, which deals with sanctions for non-compliance, expressly states that failure to comply with the Disclosure Pilot may lead to the court adjourning any hearing, making an adverse order for costs or ordering that any further disclosure by a party is conditional on any matter that the court shall specify. Furthermore, the court also has the power to deal with any failure as a contempt of court in appropriate cases, which itself carries the risk of fine or imprisonment.

II YEAR IN REVIEW

The implementation of the Disclosure Pilot on 1 January 2019 represents the most significant shake-up of the English disclosure rules since they were first launched 20 years ago. This section addresses the background to the Disclosure Pilot.

In May 2016, a disclosure working group (DWG) was set up by the then Chancellor of the English High Court in response to widespread concerns regarding the perceived excessive costs, scale and complexity of disclosure. The DWG included lawyers, experts, judges and court users. The task was to identify problems and propose a practical solution.[21] After its first meeting, the DWG concluded that 'it could not seriously be disputed that standard disclosure often produces large amounts of wholly irrelevant documents, leading to a considerable waste of time and costs [and that] inadequate judicial resources had led, on occasion, to judges not being able to deal effectively with disclosure issues at a case management conference, so that, in the absence of agreement between the parties, standard disclosure often became the default option.'[22]

Under CPR Part 31, unless the court orders otherwise, the order to give disclosure is an order to give 'standard disclosure'.[23] This means that parties are required to disclose documents on which they rely as well those documents that adversely affect their own case, adversely affect

19 'If a party cannot produce a particular document (because the document no longer exists, the party no longer has it in its possession or for any other reason) the disclosing party is required to describe each such document with reasonable precision and explain with reasonable precision the circumstances in which, and the date when, the document ceased to exist or left its possession or the other reason for non-production. If it is not possible to identify individual documents, the class of documents must be described with reasonable precision.'

20 Rule 44.2(2), CPR.

21 DWG Press Announcement, 31 July 2018: https://www.judiciary.uk/wp-content/uploads/2018/07/press-annoucement-disclosure-pilot-approved-by-cprc.pdf.

22 ibid.

23 Rule 31.5(1)(a), CPR.

another party's case or support another party's case.[24] CPR 31 does allow the court to adopt a different approach to the available options, such as disclosure on an issue-by-issue basis. However, as highlighted by the DWG, standard disclosure was usually the default position.

The DWG's view was that, while standard disclosure might be appropriate for factually complex cases, other cases could be dealt with fairly and efficiently on the basis of focused and limited disclosure. The DWG agreed that CPR Part 31 should be redrafted and that new rules should explore the option of new graduated models of disclosure and a new e-disclosure protocol taking into account likely developments in technology. On 13 July 2018, the new mandatory Disclosure Pilot was approved and subsequently launched on 1 January 2019.

III CONTROL AND PRESERVATION

Under the Disclosure Pilot, a party that knows it is or may become a party to proceedings that have been commenced, or that knows that it may become a party to proceedings that may be commenced, is required to take reasonable steps to preserve documents in its control that may be relevant to any issue in the proceedings.[25] Legal representatives are also under a duty to take reasonable steps to preserve documents within their control that may be relevant to any issue in the proceedings.[26] As noted in Section I, the definition of 'document' extends to ESI.

Control in this context includes documents (1) that are or were in a party's physical possession, (2) in respect of which a party has or has had a right to possession, or (3) in respect of which a party has or has had a right to inspect or take copies.[27]

The duty to preserve documents includes documents that might otherwise be deleted or destroyed in accordance with a document retention policy or in the ordinary course of business. In certain situations, preservation may require making a copy of sources and documents and storing them. The obligation to preserve documents requires a party to do the following:

a suspend document deletion or destruction processes for the duration of the proceedings;

b send a written notification to all relevant current and former employees that identifies the documents or classes of documents to be preserved, and notifies the recipient that he or she should not delete or destroy those documents and should take reasonable steps to preserve them; and

c take reasonable steps so that agents or third parties that may hold documents on the party's behalf do not delete or destroy documents that may be relevant to the issues in dispute.[28]

At the time of filing their particulars of claim or defence, as the case may be, a party is required to confirm in writing that steps have been taken to preserve documents in accordance with the Disclosure Pilot.

24 Rule 31.6, CPR.

25 Paragraph 3.1(1), Disclosure Pilot.

26 Paragraph 3.2(1), Disclosure Pilot.

27 Appendix 1, Disclosure Pilot.

28 Paragraph 4, Disclosure Pilot.

IV REQUESTS AND SCOPE

The court expects the parties and their legal representatives to cooperate with each other and to assist the court so that the scope of disclosure, if any, that is required in proceedings can be agreed or determined by the court in the most efficient way possible.[29] As explained in Section I, the parties are required to complete the DRD prior to the first case management conference by completing the steps identified in Paragraphs 7 and 10 of the Disclosure Pilot, which are summarised in table form in the DRD at Appendix 2 of the Disclosure Pilot. The parties' obligation to complete, seek to agree and update the DRD is ongoing. If a party fails to cooperate and constructively to engage in this process, the other party may apply to the court for an appropriate order. The court may make any appropriate order, including the dismissal of any application for extended disclosure or the adjournment of the case management conference with an adverse order for costs.[30]

Section 2 of the DRD comprises a questionnaire and requires the parties to provide information relating to all data sources to be considered at collection, such as: document repositories or geographical locations, or both; mobile phones, tablets and other handheld devices; cloud-based data storage; webmail accounts, such as Gmail and Hotmail; and third parties that may have relevant documents that are under a party's control (e.g., agents or advisers). The parties are also required to provide details regarding those sources that are unavailable but that may host relevant documents.

As required by Paragraph 9.6 of the Disclosure Pilot, where a disclosure model requires searches to be carried out, the parties are required to discuss and seek to agree the following matters that are set out in Section 2 of the DRD with a view to reducing the burden and cost of the disclosure exercise:

a that the scope of the searches that the disclosing parties are required to undertake be limited to:
- particular date ranges and custodians of documents;
- particular classes of documents or file types;
- specific document repositories or geographical locations;
- specific computer systems or electronic storage devices; and
- documents responsive to specific keyword searches, or other automated searches (by reference, if appropriate, to individual custodians, creators, repositories, file types or date ranges, or concepts);

b if narrative documents are to be excluded, how that is to be achieved in a reasonable and proportionate way;

c the use of:
- software or analytical tools,[31] including technology-assisted review software and techniques;[32] and
- coding strategies, including to reduce duplication; and

d prioritisation and workflows.

29 Paragraph 2.3, Disclosure Pilot.

30 Paragraph 10.3, Disclosure Pilot.

31 The DRD provides that: '[p]arties are to consider using the full range of tools in the analytics suite available to them (either in-house or via e-disclosure specialist firms), to assist in the review. This might include some of the more complex tools available such as technology (or computer) assisted review (TAR or CAR), and other similar software review tools…'.

32 The DRD provides that: '[p]arties are to consider the use of technology/computer assisted review tools. These are software tools used for prioritising or coding a collection of documents which take account of a

V REVIEW AND PRODUCTION

If the court makes an order for extended disclosure, this will usually include the timetable for compliance. The required time frame will depend on a number of factors, such as the nature and complexity of the case, the volume of documents involved and the time it will take the parties to comply with their obligations. These issues will have been discussed between the parties before the case management conference when they were preparing the DRD and further with the court during the hearing itself. A party always has the option of seeking a time extension at a later stage, but whether or not it will be granted will depend on the circumstances and reasons for the request.

Paragraph 9.8 of the Disclosure Pilot requires parties to have regard to the guidance contained in Section 3 of the DRD when complying with an order for extended disclosure.

Section 3 of the DRD seeks to guide parties on the collection, processing, review and production of documents. The guidance states that an appropriate methodology for a case involving ESI should always include:

a collecting documents in a way that preserves the metadata where possible;
b maintaining a 'methodology record' of each stage of the process so that the methodology can be explained to the court if necessary; and
c deduplication of the data set to the fullest extent possible.

The guidance also lists those aspects of the methodology that the parties should agree as soon as possible, such as:

a how the collection data set is to be identified and collected;
b how each party intends to use analytics to conduct a proportionate review of the data set;
c how each party intends to use technology-assisted review to conduct a proportionate review of the data set (particularly where the data set is likely to be in excess of 50,000 documents); and
d format for electronic exchange.

As to the methodology record, the guidance requires that this should include information such as:

a the document sources not considered at collection and why;
b the deduplication method applied;
c any DeNISTing applied;[33] and
d any use of clustering, concept searching, email threading, categorisation and any other form of analytics or technology-assisted review.

One of the risks inherent in any disclosure or production exercise is the inadvertent disclosure of legally privileged material. It is therefore vital that measures are agreed and put into place to ensure that this risk is minimised. This will include detailed consultations between a

senior lawyer's review and judgments on a set of documents and then extrapolate those judgments to the remaining document collection'. It also requires parties to explain why they have decided not to use these tools in circumstances where they have considered them.

33 As indicated in the guidance: 'DeNISTing is a method of reducing the number of documents subject to lawyer or computer review by removing file types that are highly unlikely to have evidentiary value.'

party and its legal representative to ensure that all potential sources of privileged material are identified, agreeing appropriate searches with a view to identifying such documents, and carrying out second or even third pass reviews.

Once the documents have been produced by the parties, the receiving party may challenge the disclosure on the ground that the disclosing party has failed to comply with the terms of the court's order. Ultimately, the court may order the disclosing party to redo any aspect of its disclosure if necessary. Furthermore, as noted in Section I, 'Costs', the court may apply sanctions on the breaching party, such an adverse cost order.

VI PRIVACY ISSUES

When discharging their disclosure obligations, parties should always be mindful of their duties under any applicable data privacy laws. The key piece of legislation in England is the European Union's General Data Protection Regulation[34] (GDPR), which took direct effect in England on 25 May 2018. The GDPR regulates the 'processing' of 'personal data' and applies to both 'data controllers' and 'data processors' of personal data located in the European Economic Area (EEA).

Personal data is any information that relates to an identified or identifiable living individual such as name and surname, home address or email address. Processing includes the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data. A data controller is someone who determines the purposes and means of processing personal data, whereas a data processor is responsible for processing personal data on behalf of a data controller.

Accordingly, the preservation, collection, processing, review and production of ESI by a party or its legal representatives in the context of disclosure is likely to constitute the processing of personal data by a data controller (the party) and potentially a data processor (the legal representative or any third party retained for disclosure purposes). Therefore, a party will need to ensure that it complies with its obligations under the GDPR before it processes any personal data.

The GDPR contains seven key data protection principles that a data controller must comply with. The first principle requires personal data to be processed lawfully, fairly and in a transparent manner in relation to individuals. There are six lawful bases for processing that are set out in Article 6 of the GDPR. At least one of them must apply. Three of the most relevant bases for disclosure are: (1) where the individual has given clear consent for a party to process their personal data for a specific purpose; (2) where the processing is necessary for a party to comply with the law (not including contractual obligations); and (3) where the processing is necessary for a party's legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data, which overrides those legitimate interests. The data controller will still need to comply with its other obligations under the GDPR even if the processing is deemed lawful.

34 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

The GDPR also imposes restrictions on the transfer of personal data outside the EEA. However, the transfer will be permitted where:

a the proposed transfer is covered by an 'adequacy decision' of the European Commission, which is a finding that the legal framework in place in that country, territory, sector or international organisation provides adequate protection; or

b the transfer is made subject to appropriate safeguards, which are listed in the GDPR.

Examples of appropriate safeguards include:

a binding corporate rules that represent an internal code of conduct operating within a multinational group and that apply to restricted transfers of personal data from the group's EEA entities to non-EEA group entities; or

b a contract between the sender and receiver that incorporates standard data protection clauses adopted by the European Commission known as the standard contractual clauses or model clauses.

VII OUTLOOK AND CONCLUSIONS

By far the most significant recent development in England has been the introduction of the new Disclosure Pilot. While it is too early to say what impact the new rules will have, it is clear from the terms of the Disclosure Pilot that parties will be required to be much more proactive in discharging their disclosure obligations and from a much earlier stage in the legal proceedings. The courts will be keen to ensure that disclosure is directed to the issues in the proceedings and that the scope of disclosure is not wider than is reasonable and proportionate[35] to resolve those issues fairly, and specifically the issues for disclosure.[36] Furthermore, for the first time, the duties of the parties and their legal representatives are clearly set out in Paragraph 3 of the Disclosure Pilot, such as the requirement to act honestly in relation to the process of giving disclosure and reviewing documents disclosed by the other party and to use reasonable efforts to avoid providing documents to another party that have no relevance to the issues for disclosure in the proceedings. It will be interesting to see what impact the new regime will have on disclosure and whether or not it will address the perceived deficiencies of the old regime.

35 As defined in paragraph 6.4 of the Disclosure Pilot.

36 Paragraph 2.4, Disclosure Pilot.

Chapter 7

FRANCE

Olivier de Courcel[1]

I OVERVIEW

At common law, a party to a lawsuit may request the opposing party to provide information or materials in relation to their dispute and the latter must provide them, even if it considers them unfavourable to its case. Thus, a pretrial discovery phase is launched with a variety of means of communication, such as interrogations, depositions, applications for admission and requests for the production of documents.

In the United States, companies must, in general, preserve any document that may be relevant in anticipation of or in the conduct of a lawsuit.[2] In a dispute, each party must systematically disclose a copy or a description of all documents and electronically stored information that it may use in support of its claim or defence. Lastly, such party may request and obtain the same materials from the opposing party in as far as relevant to the opposing party's claim or defence and proportional to the needs of the case.[3]

In France, as in other civil law jurisdictions, there is no straightforward equivalent to this notion and process of discovery. According to Article 9 of the Code of Civil Procedure (CPC), in general, it is up to each party to provide evidence of the 'facts necessary for the success of its claims'. In addition, as soon as a party cites a document, it must immediately communicate it to the other parties. Such party is not, however, also required to immediately disclose all the elements likely to serve as evidence in the dispute in question. Lastly, a party may request documents from the other party, but the communication of such documents must then be decided by a judge order (the equivalent of a *subpoena duces tecum*). This communication may be subject to a day penalty in an amount that the judge's order will fix.

The judge is in charge of controlling the timing of the proceedings. Before concluding the preliminary pretrial phase, he or she may invite the attorneys to reply to the pleas on which they have not concluded, or to provide the factual and legal explanations necessary for the settlement of the dispute. In these circumstances, if a party does not produce the requested documents, the judge will draw the appropriate conclusions for the resolution of the dispute.

Finally, the judge, on his or her own initiative or at the request of a party, may order an investigation measure, such as a judicial expertise, the production of affidavits or the hearing of witnesses. This type of measure may be ordered before the trial if there is a legitimate reason to preserve or establish evidence of facts on which the resolution of the dispute may depend (CPC, Article 145). The aim is to improve the applicant's 'probationary situation' – in other

1 Olivier de Courcel is a partner at Féral-Schuhl / Sainte-Marie.

2 US Federal Rules of Civil Procedure, Rule 37 (e).

3 ibid., Rule 26 (a)(1)(B) and Rule 26 (b)(1).

words, to establish proof of facts that the applicant is not in a position to establish totally or alone. The judge may also order such a measure during the trial itself, if the party alleging a fact does not have sufficient evidence to prove it. But, in such a case, the measure must not make up for this party's failure to provide evidence (CPC, Article 146).

In all cases, each party will bear its own costs for the production of evidence until the judge makes his or her decision and decides on the burden to pay for the costs of the trial.

In the context of civil procedure, as there is no general obligation to disclose documents in anticipation of a trial, there is also no general obligation to preserve evidence (including to store and back up electronic data) for possible trials. However, there are special texts that impose retention periods for certain types of documents in view of procedures that are subject to administrative or criminal sanctions. In this area, recent developments in digitisation and archiving, investigation techniques and digital surveillance (e.g., interception of electronic communications, collection and production of data on the technical features of communications or identifying the authors or receivers of communications) make it possible to draw a parallel with the Anglo-Saxon practice of e-discovery (see Section III).

II YEAR IN REVIEW

In the field of criminal and administrative proceedings, the rules on disclosure of electronic evidence held by third parties (most often providers of computing services or electronic communications) are undergoing significant development with the draft EU 'e-Evidence' Regulation, dated 17 April 2018.[4]

The aim of this proposed Regulation is to facilitate the collection of electronic evidence for the purposes of criminal and anti-terrorism investigations and prosecutions. The European Commission observed that in more than half of criminal investigations, judicial or police authorities request access to electronic evidence held by service providers established in another Member State or outside the European Union. According to the Commission, for almost two-thirds of offences, cross-border investigations or prosecutions cannot be carried out properly, mainly because of the time required to collect such evidence or because of the fragmentation of the legal framework.[5]

Similar difficulties were resolved in the United States by the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), promulgated on 23 March 2018 following a dispute between Microsoft and the Federal Bureau of Investigation in an investigation involving emails stored in Ireland.[6]

If adopted, the e-Evidence Regulation will create a uniform procedure to require a service provider to retain or produce data that it stores, even if the data is stored in a country other than the one in which the investigation or prosecution is carried out. This mechanism will apply to all types of digital service providers established in the European Union, including providers of electronic communications services, social networks, online markets, hosting services and internet infrastructure.

4 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).

5 European Commission, 'Security Union: Commission facilitates access to electronic evidence' Press release, dated 17 April 2018.

6 United States Supreme Court, *Microsoft Corp v. United States*, 17 April 2018.

All injunctions issued under this procedure will have to be issued or validated by a judicial authority of a Member State as part of criminal proceedings, during the pretrial investigation phase or during the proceedings. An injunction may only be issued after an assessment of its proportionality and necessity in the particular case under consideration.

III CONTROL AND PRESERVATION

French civil procedure law does not impose a general obligation to keep documents in anticipation of or in the conduct of a trial. It is up to the judge to decide, on a case-by-case basis, whether documents requested by one party should be preserved and communicated by the other.

Even in the absence of a positive duty to keep documents, safeguarding relevant documents in view of litigation risks would seem a matter of basic prudence and business judgement. This requires that documents be kept for the duration of the limitation period applicable to their subject matter. Therefore, corporate document archiving and retention policies usually provide for retention periods adapted to the different limitation periods, with five years being the time bar applicable by default.

In this regard, a decision of the Paris Court of Appeal in the field of antitrust law referred to a 'general duty of prudence' on the part of any company under investigation by the Competition Authority, 'to preserve any evidence likely to enable [such company] to justify the lawfulness of its practices'.[7] This duty to keep records concerns 'not only the accounting documents and supporting documents provided for in Article L. 123-22 of the French Commercial Code, but also all evidence of the lawfulness of [its] commercial practices . . . until the expiry of the limitation period or a decision to dismiss the case'. Such a general duty of prudence is similar to the preservation requirement of discovery.

In any event, before a trial, a plaintiff may apply to the judge for an order for any legally admissible investigation measure, including requiring the opposing party or a third party to disclose evidence in view of a trial (CPC, Article 145). Although there is no notion of 'possession, custody or control' over documents as under common law, the judge will assess whether the measures requested are legally admissible. For example, it may be a legally permissible measure to require the publisher of a website to provide the IP address of an internet user whose message it has received on its website.[8]

Moreover, although the rules of civil procedure do not impose a general obligation to preserve evidence in anticipation of a trial, some special texts require certain types of documents to be preserved for specific periods of time. For example, for companies and other traders, the Commercial Code (Article L. 123-22) requires that accounting documents and supporting documents be kept for 10 years. It also specifies the conditions for the presentation and storage of these documents.

Tax law extends this obligation by introducing mandatory methods and retention periods for invoices and other supporting documents and explicitly refers to documents in electronic form.[9] In this respect, the Tax Administration specifies that 'the failure to keep

7 Paris Court of Appeal, 26 January 2012, No. 10/23945.

8 Paris Court of Appeal, 11 June 2004, D. 2004. IR 2893.

9 Article L. 102 B et seq. of the Tax Procedures Book.

records, whether totally or partially, noticed by the administration's agents may therefore be sanctioned. For example, failure to keep original invoices in electronic form may lead to the VAT deductions being repelled.'[10]

In other specific areas, special texts provide for similar obligations to keep documents for a fixed period of time, including in electronic form. Thus, in labour law, such an obligation applies, for example, to the single personnel register and to employers' declarations of accidents at work.[11]

In principle, a party to a civil case cannot rely on the special texts to request the evidence they provide for. An exception is made, however, to allow the disclosure of accounting documents in court: a party may request the judge to order their disclosure in cases of succession, community, company sharing, judicial reorganisation or liquidation.[12]

Under ordinary law, failure to keep documents is not punishable. An exception is made under criminal law for intentional destruction of documents that were likely to result in the discovery or proof of a criminal offence.[13] The punishment is three years' imprisonment or a €45,000 fine, or both. However, some special texts provide for specific sanctions, including the General Tax Code, which expressly provides that:

> *The refusal to disclose documents and information requested by the administration in the exercise of its right of disclosure or any conduct that obstructs disclosure shall result in the application of a fine of 10,000 euros. This fine shall apply for each request, as soon as all or part of the requested documents or information is not disclosed. A fine of the same amount shall apply in the event of failure to keep these documents or of destruction before the prescribed deadlines.*[14]

IV REQUESTS AND SCOPE

In the absence of a procedure equivalent to discovery, the parties to a trial do not have to agree in advance on the evidence they will produce: each party produces the evidence in support of its claims and, if it wants to obtain other materials from its opponent, this will only happen pursuant to the judge's request.

The courts are called upon to assess the proportionality of the disclosure requested, considering not just the interest of the applicant, but also the protection of fundamental freedoms (in particular the right to privacy) and secrets protected by law (in particular professional and business secrecy).

A frequent example of this proportionality test concerns disputes between employees and employers, where the courts make a distinction between the types of documents that employers can produce from their information systems. Documents contained on an employee's computer are presumed to be of a professional nature. However, to respect employees' right to privacy, which also applies in the workplace, an employer will not be able to validly avail itself of documents that have been expressly designated as personal or private by the employee.[15]

10 Official Bulletin of Public Finance-Taxes: BOI, CF-COM-10-10-30-10-20180720, § 290, 20 July 2018.

11 Labour Code, Articles R1221-26 and D4711-3.

12 Commercial Code, Article L123-23.

13 Penal Code, Article 434-4.

14 General Tax Code, Article 1734.

15 Court of Cassation, 2 October 2001, Social Chamber, Appeal No. 99-42942.

In the field of intellectual property, when evidence of counterfeiting is being sought, the right holder may request a court order to carry out an infringement seizure. A bailiff will then be able to enter any place where the infringement can be detected and to seize all accessible evidence, such as samples of alleged infringing objects or financial information on the commercial exploitation of these objects, including any documents stored electronically. Where the infringement concerns a computer program or a database, the judge may simply order a copy.[16]

Before launching a trial, a party may also ask the judge for an investigation measure known as *in futurum*. The request must be based on a legitimate ground, which will be assessed at the discretion of the judge,[17] and must seek a 'legally admissible investigation measure' (e.g., judicial expertise, production of affidavits, hearing of witnesses), in accordance with the requirements of the CPC.[18]

In this context, the judge will apply the proportionality test in accordance with French rules. For example, he or she may put aside professional secrecy or attorney–client privilege not applicable under French law.[19] According to the same rules, case law prohibits investigation measures that are general,[20] such as investigation measures that, in a case in 2012, 'authorised the bailiff to seize any social, fiscal, accounting or administrative document of any nature whatsoever and allowed him to search at his own discretion the company's premises [subject to the investigation measures]'.[21] More specifically, judges exclude measures that exceed the needs of the case and whose purpose is not limited in space and time.[22]

In addition to the principle of proportionality, case law also imposes a principle of fair evidence. In short, in a civil trial the parties will only be able to rely on evidence obtained fairly, whereas before a criminal judge, a party will be able to rely on evidence that has been illegally obtained, as long as that evidence has been open to debate in a fair trial.[23] Practically, this distinction may lead to the exclusion, before the civil court, of private data recordings made by one party without the knowledge of another,[24] which constitutes an unfair process and is therefore not admissible as evidence (but would be admissible before a criminal court).[25] This only concerns evidence used by the parties: in criminal cases, investigators must comply with the principle of fair evidence.[26]

16 Intellectual Property Code, Article L332-4.

17 Court of Cassation, 12 July 2012, Civil Chamber 2, Appeal No. 11-18.399.

18 Code of Civil Procedure, Article 145. See Section I, above.

19 Court of Cassation, 3 November 2016, Civil Chamber 1, Appeal No. 15-20.495.

20 Court of Cassation, 7 January 1999, Civil Division 2, Appeal No. 97-10.831.

21 Court of Cassation, 16 May 2012, Civil Division 2, Appeal No. 11-17.229.

22 Court of Cassation, 14 November 2013, Civil Chamber 2, Appeal No. 12-26.930.

23 European Court of Human Rights, 12 July 1988, *Schenk v. Switzerland*, Application No. 10862/84; Cass. Crim. 15 June 1993: Bull. Crim, No. 210; Cass. Crim. 27 January 2010, No. 09-83.395 'no legal provision allows criminal judges to exclude evidence provided by an individual to the investigation services solely on the ground that it was obtained unlawfully or unfairly and that it is for them alone, pursuant to article 427 of the Code of Criminal Procedure, to assess its probative value, after having submitted it to the adversarial discussion.'

24 'Criminal judges may not dismiss evidence produced by the parties on the sole ground that it has been obtained unlawfully or unfairly.' (Cass. Crim., 26 April 1987).

25 Dictionnaire de la justice, PUF, 'Proof', X. Lagarde. The principles of civil procedure also cover competition law (Cass. Ass. Plén, 7 January 2011, Nos. 09-14.316 and 09-14.667).

26 Cass. Crim. 17 March 2015, No. 14-88.351 (on the sound system of a police custody cell to obtain evidence in matters of organised crime).

The field of criminal procedure is most concerned with electronic evidence, and the means of accessing this evidence have been strengthened on the grounds of the fight against terrorism.[27] Electronic evidence can be searched for via subpoena procedures (e.g., for technical records or location data) as well as search and seizure procedures (which allow access to content data). Specifically, the CPC allows investigators to access data from a computer system located on the premises where the search takes place. The search may also cover data stored in another computer system, 'as long as such data is accessible from the initial system or available to the initial system'. However, the CPC reserves the duty to comply with international treaties, which govern the authorities' access to data collected when it is stored in another computer system located outside the national territory.[28]

V REVIEW AND PRODUCTION

As French civil procedure law does not provide for a general obligation to communicate to the opposing party the documents relevant to the dispute, the use of tools for mass document analysis (e.g., technology assisted review or predictive coding) remains limited to specific categories of litigation.

For instance, the question of mass data review is an important aspect of investigations into antitrust practices.[29] Competition Authority investigators may require disclosure and obtain or make copies, by any means and using any medium, of books, invoices and other professional documents of any kind, in any hands. With regard to electronic documents, they 'have access to software and stored data as well as to the restitution in clear text of information likely to facilitate the performance of their missions. They may request the transcription by any appropriate processing of documents directly usable for control purposes'.[30]

These provisions do not allow investigators to request, in a general and imprecise manner, all documents located in the company's computers. However, case law has specified that 'this limitation to the powers of investigators cannot be interpreted as requiring them to know a priori the existence and name of each of the documents communicated, since this information is, by definition, known only by the user of the computer workstation'.[31] Therefore, the documents requested should be sufficiently identified. In this instance, evidence retrieval software (forensic software) can, and should, be configured to extract only documents relevant to the case. In this context, however, the Court of Cassation specified in late 2018 that government entities may seize a whole mailbox, because email files cannot be split.[32]

27 Law No. 2014-1353 of 13 November 2014 on the fight against terrorism; Law No. 2016-731 of 3 June 2016 strengthening the fight against organised crime, terrorism and their financing, and improving the efficiency and guarantees of criminal procedure.

28 Code of Criminal Procedure, Article 57-1.

29 Other specific areas regulated by supervisory authorities have similar developments in the right of investigators to communicate: see, for example, in the pharmaceutical sector (Public Health Code, Article L. 1421-3; in matters of consumer protection (Consumer Code, Article L. 512-11); and in financial control (Code of Financial Courts, Article R. 241-1 et seq.).

30 EU Directive 2016/943 of 8 June 2016, transposed into the Commercial Code, Article L. 450-3 and L. 450-4.

31 Paris Court of Appeal, Pôle 5, Chamber 7, 26 October 2017, No. 17/01658.

32 Court of Cassation, Criminal Division, 19 December 2018, No. 17-87357: in 'the making of global and undifferentiated seizures of electronic mail files and global seizures of electronic mail files, it is consistently the case that an Outlook-type e-mail file, unless its content is altered, is unbreakable'.

At a second stage, given the ultimately broad scope of a company's data that government entities may seize or copy, the question arises as to which of these data are then admissible as evidence. The prosecutors must indeed sort out the materials obtained as a result of pretrial investigations before submitting them to trial.

In this respect, in France, as elsewhere, attorney consultations, attorney–client correspondence and meeting notes are covered by attorney–client privilege and are inadmissible, whether they appear on paper or in electronic format. The same applies to correspondence between the company's attorney and his or her fellow attorneys (except when marked 'official') or with a foreign attorney.

Nevertheless, case law specifies that:

> *this principle is not absolute and has several exceptions; thus, by way of illustration, it cannot be accepted that exchanges between two correspondents with copy to an attorney may benefit from the legal privilege applicable to the confidentiality of attorney/client correspondence unless this legal privilege is distorted; that indeed, it would then be sufficient for a company to exchange e-mails with another company with a recipient who would be qualified as an attorney in order for any correspondence to benefit from this legal privilege.*[33]

Similarly, the principles of secrecy of correspondence and fair evidence may be relied upon by a party in civil matters, as illustrated by an appeal decision overturning an investigation measure that made it possible to extract from a former employee's computer – using forensic software – documents likely to establish proof of unfair competition but recorded in the employee's personal email files.[34] Indeed, documents identified as personal cannot be opened without the employee having been duly called and having been able to attend if he or she so wished.

Finally, an EU Directive of 8 June 2016, transposed in France by an act of 30 July 2018, introduced into French law a definition of 'business secrecy' and a legal regime to protect it.[35] Before this Act, a party could ask the civil judge to order an investigation measure, if necessary in a non-adversarial manner (CPC, Article 145), to limit the risk of concealment of evidence, and to put in escrow the evidence obtained, even though it could be protected by business secrecy. The new legal regime of business secrecy will necessarily have an effect on the implementation of such investigation measures.

VI PRIVACY ISSUES

E-discovery proceedings brought by companies or authorities located outside the European Union against French companies necessarily involve the transfer of personal data (e.g., the communication of emails). This raises difficulties with regard to legislation on personal data.

Both the EU General Data Protection Regulation (GDPR) and the French Computer and Freedoms Act[36] prohibit, in principle, the transfer of personal data to countries whose

33 ibid.

34 Court of Appeal of Versailles, 12th Chamber, 24 June 2014, No. 12/02820. See Section IV, above.

35 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and commercial information (trade secrets) against unlawful acquisition, use and disclosure; transposed into Articles 151-1 et seq. of the Commercial Code.

36 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such

legislation does not offer an equivalent level of protection. To derogate from this prohibition, specific compliance mechanisms must be put in place to provide the framework for each envisaged cross-border data transfer. Such mechanisms include adherence to the standard contractual clauses published by the European Commission, establishing binding corporate rules for intra-group transfers or adhering to a code of conduct.

On this basis, French companies have already refused in the past to follow a discovery request, arguing that the disclosure outside the European Union of documents containing personal data is prohibited by French law.[37]

This issue is now addressed by Section 48 of the GDPR, which states that:

> *Any decision of a court or government entity of a third country requiring a Data Controller or Data Processor to transfer or disclose personal data may not be recognised or made enforceable in any way unless it is based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer under this Chapter.*

Therefore, any request for discovery must be made within the framework of a treaty, in this case an international mutual legal assistance treaty. In France, as in the United States and elsewhere, the applicable procedure consists of international rogatory letters as provided for by the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters (the Convention). This procedure allows any judge of a state party to the Convention to request, in accordance with the terms of its legislation, the competent authority of another state party to carry out any investigation measures. International rogatory letters are issued and received in each country through a central authority, which acts as a 'one-stop shop'.

In the context of the Convention, France has declared that it will not execute international rogatory letters issued in common law countries for the purpose of obtaining evidence before a trial (i.e., pretrial discovery), unless the documents required are listed restrictively and have a direct and precise relationship with the subject matter of the proceedings.

Since the 1987 Supreme Court Aérospatiale judgment,[38] US courts have considered civil judicial cooperation proceedings under the Convention to be optional – that is, not replacing the extraterritorial application of the US pretrial discovery rules.

Regardless of whether the framework of the e-discovery procedure is national or international, the GDPR protection principles will consist essentially of data limitation and of proportionality (i.e., they will require that only personal data necessary for the procedure be disclosed).

The French Data Protection Authority and the European Coordination Committee recommend in this respect to (1) provide anonymised or pseudonymised data, where possible; and (2) request (via 'stipulative court orders') to limit the scope of the documents

data, repealing Directive 95/46/EC (General Data Protection Regulation), Article 45 et seq.; Law 78-17 of 6 January 1978, Articles 68 and 69.

37 See, for example, *In re Activision Blizzard, Inc*, 86 A.3d 531 (2014) (Del. Ch. 21 February 2014).

38 United States Supreme Court, *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, No. 85-1695, 15 June 1987, 482 U.S. 522 (1987).

to be communicated, to specify the conditions related to the use and communication to third parties of the personal data collected, and to provide for the security and confidentiality measures to be followed.[39]

The same authorities recommend, for companies that may be subject to an e-discovery procedure (e.g., French subsidiaries or parent companies of corporate groups with a company located in the United States), that these procedures be adapted to comply with the GDPR. For example, companies can:

a provide for an express information notice to employees (in an IT charter, for example) on the possibility that their data may be transferred outside the European Union in such a situation;

b equip themselves with software tools to 'filter' personal data, to be able to communicate only those data that may be required for an e-discovery procedure, should this happen; and

c insist that employees expressly identify their personal files (using an explicit name: 'personal' or 'private'), to be able to exclude them from the documents to be communicated.[40]

In all cases, the persons whose data are communicated shall retain their rights over such data, namely rights of access, objection, deletion and limitation. US courts have previously accommodated these types of rights, despite normally taking a different view on the right to privacy.[41]

In view of the extraterritorial and intrusive nature of cross-border discovery procedures, the French authorities have adopted a blocking statute[42] designed to prevent, in particular, 'fishing expeditions' (i.e., procedures for economic intelligence purposes). As amended in 1980, this statute prohibits both the request and disclosure of any 'documents or information of an economic, commercial, industrial, financial or technical nature intended to constitute evidence for or in connection with foreign judicial or administrative proceedings' if outside international judicial cooperation mechanisms.[43] The statute applies even if the search for information is not followed by a trial and even if the person being prosecuted is neither French nor a French resident. Violations of this statute are subject to criminal sanctions.

To date, there has been only one conviction in France, in 2007, against a lawyer who had sought information from a company director for a lawsuit in the United States by making false suggestions as to the nature of the evidence he was asking for.[44] On the US

39 French Data Protection Authority, Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as 'Discovery'; G29, WP 258, Working Document 1/2009 on pretrial discovery for cross-border civil litigation.

40 The New York City Bar has released similar guidelines to help US companies anticipate the conflict of laws between discovery procedures and privacy laws: 'Cross-Border E-Discovery: Navigating Foreign Data Privacy Laws and Blocking Statutes in U.S. Litigation' (16 July 2018).

41 ibid., footnote 37.

42 Law No. 68-678 of 26 July 1968 on the communication of documents and information of an economic, commercial, industrial, financial or technical nature to foreign natural or legal persons.

43 ibid., Article 1 *bis*.

44 Paris Court of Appeal (9th Chamber B), 28 March 2007; confirmed by the Court of Cassation, Criminal Chamber, 12 December 2007, No. 07-83.228.

side, the courts refuse to automatically follow French litigants on this legal basis. Following the Supreme Court, they balance the interests in question in order to define the scope of discovery.

A draft reform of the blocking statute is expected in the coming year. The issue of its international effectiveness will likely be one of the points of attention.

VII OUTLOOK AND CONCLUSIONS

Although French law does not have discovery (and e-discovery) procedures, several factors are indicating a move in this direction and should be closely monitored.

The texts governing areas that are subject to government control (e.g., tax law, antitrust law, financial markets, criminal investigations) allow for the seizure of a wider scope of evidence than that available to private persons in civil matters. Digital data are collected in bulk (big data) and the government regulators increasingly use electronic evidence retrieval software to sort them.

Similarly, in the context of investigations and prosecutions in criminal and antiterrorism matters, the draft e-Evidence Regulation (see Section II) should have a significant impact on the taking of electronic evidence. If it enters into force, it will make it easier for judges to require a service provider to retain or produce data stored by it, even when the data is stored in another country. This legislative initiative is in line with the executive agreements promoted by the US CLOUD Act to allow such cross-border injunctions without going through the international rogatory letters provided for by mutual legal assistance treaties (in the case of France, the 1970 Hague Convention).

With regard to civil procedure, the new statutory regime defining and specifying the protection of business secrecy, introduced into the Commercial Code in 2018, should have a significant impact on the production of documents by businesses, as well as on the investigation measures businesses may request from a judge.

Chapter 8

JAPAN

Kentaro Toda[1]

I OVERVIEW

The Japanese legal system is based on civil law and courts render decisions based on the primacy of codified law. As opposed to common law systems, such as in the United States, there is less emphasis on judicial precedents that judges use as bases to rule in subsequent cases. Japan has a unified court system, of which the highest level is the Supreme Court. There are no separate and discrete state court systems. There are generally three tiers of courts, with actions first filed in a court of first instance, followed by an intermediate appeal to one of eight high courts, followed by an appeal to the Supreme Court.

There is no discovery procedure under Japanese civil procedure laws. Parties are required to obtain evidence to establish or disprove the merits of the plaintiff's claim of their own accord. Each party is therefore required to evaluate and prepare its claims based on the evidence each of them has in its possession. This differs significantly from US civil procedure rules, which call for lengthy discovery periods where the parties are able to seek and obtain information and evidence related to the claims at issue from the opposing party. As there is no discovery procedure in Japan, there is no electronic discovery procedure either. To collect electronically stored information (ESI) under the control of the opposing party or a third party, a party must utilise evidence collection methods permitted under the Code of Civil Procedure (see Section IV).

II YEAR IN REVIEW

Although the legal system does not provide for the collection or disclosure of ESI, the government has been discussing ways to develop the use of technology in court procedures. The courts do not allow parties to file submissions online; rather, all documents are submitted in hard copy. However, in 2017, the government established a committee to evaluate how courts can update the technological processes of their civil law procedures. In March 2018, the committee issued a report with its recommendations regarding how to integrate electronic tools into the civil court process. The report focuses on three improvements:

a e-filing: filing of complaints and arguments electronically, rather than solely by hard copy;

b e-court: using web conference systems to enable the parties to participate in meetings with courts over the internet; and

1 Kentaro Toda is a partner at TMI Associates.

c e-case management: accessing court submissions, such as complaints, arguments and evidence, over the internet.

To implement the systems listed above, the committee is considering a three-phase implementation process:

a Phase 1: commencement of the operation of a web conference system and videoconferencing, which will be possible under current laws without any amendments. These changes can be implemented relatively quickly by acquiring new equipment, such as web conference systems.

b Phase 2: revisions to relevant laws and regulations, which will allow other portions of the recommendations to be implemented.

c Phase 3: construction of remaining systems and receipt of user feedback, including from those who have experienced issues with IT systems.

III CONTROL AND PRESERVATION

As mentioned in Section I, there is no discovery process in Japan. In general, parties do not have any duty to preserve ESI under the Code of Civil Procedure, as each party is required to obtain relevant evidence on its own. Because there is no duty to preserve, there are no sanctions for failure to do so. However, by utilising the methods explained in Section IV, the parties will be able to obtain documents from the opposing party.

IV REQUESTS AND SCOPE

If a party wants to obtain evidence from the opposing party or a third party, it must try to utilise the collection methods permitted under the Code of Civil Procedure, set forth below.

i Preservation of evidence

Preservation of evidence is a legal proceeding to examine and preserve evidence that might become impossible or difficult to examine by the time the actual hearing is held. It is possible to preserve evidence before a lawsuit is filed, and any kind of evidence, including electronic data, can be subject to this procedure. The party must provide written reasons for why they need to preserve the evidence and why the evidence needs to be examined when the actual hearing is going to be held.

ii Petition for an order to submit a document

A party may file a petition with the court to order the opposing party or a third party to submit a document, by explaining the necessity of the petition. The party must also describe the following in the petition:

a an indication of the document;

b the purport of the document;

c the holder of the document;

d the facts to be proven by the document; and

e the grounds for the obligation to submit the document.

If the court finds that there are legitimate grounds to grant the petition, it will issue the order. In some past cases, courts have determined that documents should be disclosed in electronic form and have accordingly ordered the document holder to disclose the ESI itself.

V REVIEW AND PRODUCTION

The Code of Civil Procedure does not have any rules regarding the use of advanced analytical tools to facilitate analysis of produced materials. However, in situations where parties have the opportunity to analyse ESI on their own, these tools are popular.

There is no attorney–client privilege or work-product doctrine protecting the confidentiality of certain documents. However, in the competition law area, there has been some discussion on introducing attorney–client privilege in relation to investigations by the Japan Fair Trade Commission. The Cabinet recently approved this through the amendment of regulations and drafting of new guidelines. This is limited to the competition law area, but nonetheless represents a large step forward for the legal system.

VI PRIVACY ISSUES

The Act on the Protection of Personal Information (APPI), which was introduced in 2003, regulates the protection of personally identifiable information. Amendments were introduced to the APPI in September 2015, which were fully implemented on 30 May 2017. The APPI requires companies to obtain consent to process personal data, unless any of the exceptions permitted under the law are applicable.

When the parties plan to provide documents or ESI containing personal data to the court, the APPI will apply. Under the APPI, parties are generally prohibited from providing personal data to the court without consent; however, it allows the provision of personal data without consent if the 'personal data is necessary for the protection of the life, body, or property of an individual and if it is difficult to obtain the consent of the person'. A party will be able to provide personal data to the court if this exception applies.

In addition, there are cases when a company is asked by the court of a foreign country, or by the parties to foreign litigation themselves, to produce documents or data that contain personal information. Under the APPI, if personal data is to be transferred to third parties in a country outside Japan, a requirement is imposed to obtain the prior consent of the relevant individuals. If the company does not receive consent, which is normally the case, it should consider whether an exception to the rule applies.

VII OUTLOOK AND CONCLUSIONS

As mentioned in Section I, there is no discovery process in Japan, and parties are required to obtain evidence on their own to establish or disprove the merits of the plaintiff's claim. There is currently little to no discussion regarding changes to this basic structure. It is very unlikely that a discovery process similar to that of the United States will be introduced in the near future.

However, because of the importance of ESI in terms of economics and business transactions, it is becoming increasingly important to have a system that allows parties to effectively collect and submit ESI. As mentioned in Section II, the government has been discussing technological updates to civil law procedures, which should be closely monitored.

Chapter 9

POLAND

Anna Kobylańska, Marcin Lewoszewski, Krzysztof Muciak and Maja Karczewska[1]

I OVERVIEW

In general, Poland has not adopted the concept of e-discovery as it is understood in common law jurisdictions, such as the United States. However, collecting and using evidence for criminal or civil proceedings is regulated in detail under Polish law. The case law related to evidence as such is also broad and has a long history.

There are some provisions of Polish law that relate to the use of electronically stored information (ESI), as detailed in Section II.

In addition, practitioners have a well-established view in relation to collecting and using electronic evidence from the perspective of privacy regulations. These regulations are the main concern for businesses when it comes to, for example, investigations connected to employment matters.

II YEAR IN REVIEW

Amendments to the Code of Civil Procedure (CPC) came into force in 2016, which specified that electronic documents are explicitly allowed as evidence in civil proceedings, and in many cases this evidence may be of even greater importance than standard, physical evidence.

According to Article 243(1) of the CPC, to classify a material as a document, the issuer of the document ought to be identifiable (by means of a signature or other identifying mark). If the issuer cannot be identified, the evidence will be classified as 'other evidence' as defined in Article 309 of the CPC (see below).

The rules applying to electronic documents as evidence generally do not differ from the general provisions on evidence. However, pursuant to Article 254 Section 2(1), an issuer of an electronic document may be, when necessary, requested by the court to provide it with the data carrier on which the document is stored. Section 2(2) of the same Article provides an exception to the obligation to present a data carrier for certain categories of witnesses who would be legally allowed to refuse to answer a question regarding the source of the electronic document – for example, whether it was created on the data carrier or uploaded there by the witness (this relates in particular to family members, who may refuse to testify in their relative's case).

The aforementioned 'other evidence' has the same evidential value as other types of evidence. The courts have expressly determined, among other things, that a print screen or

1 Anna Kobylańska and Marcin Lewoszewski are partners, Krzysztof Muciak is an advocate and Maja Karczewska is an advocate trainee at Kobylańska & Lewoszewski Kancelaria Prawna Sp. j.

an email[2] that does not contain a signature[3] shall be treated by the courts as other evidence. However, this does not prevent parties to the proceedings from presenting other materials as evidence, if it helps them prove their case. Judgments that refer to new kinds of electronic evidence can be expected.

The admissibility of electronic evidence is not questioned in criminal proceedings. The CPC does not provide definitions of 'electronic document' or 'electronic evidence', which could be further developed in the courts' decisions. In Polish legal literature, some classifications of electronic evidence used in criminal proceedings are being created and developed. However, criminal law – similar to civil law – applies the principle of free assessment of evidence, therefore these classifications will mostly be theoretical.

There are no specific rules for collecting electronic evidence. At the time of writing, there have been no announced changes to policy or legislation regarding electronic evidence in civil or criminal proceedings.

III CONTROL AND PRESERVATION

The law does not provide for e-discovery obligations related to the preservation of ESI. There are provisions of law that relate to destroying or hiding evidence that is necessary for legal proceedings, which apply to all types of evidence.

Under the Code of Criminal Procedure, any user of a device containing digital data or a computer system in which data is stored, including correspondence sent via email, is obliged to hand it over to a court or prosecutor, or – in urgent cases – at the request of the police or other authority (if the data constitutes evidence in a given case). If an individual does not voluntarily hand over evidence, the evidence can be taken by the appropriate authority by force. To detect or seize electronic data that may constitute evidence, relevant authorities (including the police) can search the premises and other places where there are reasonable grounds to believe that the data could be there.

Offices, institutions and companies conducting telecommunications activity are required to secure, at the request of a court or the public prosecutor, for a period not exceeding 90 days, digital data stored on their devices (including data on storage media and in computer systems). They must secure the data in a way that prevents it from being deleted and enables it to be easily handed over at the request of a court.

Any person who hinders or prevents criminal proceedings by concealing, destroying or distorting evidence (including destroying digital data), may be subject to criminal sanctions, including imprisonment for up to five years. Destruction of evidence is any act that prevents judicial authorities from discovering a crime or proving that the perpetrator is at fault.

IV REQUESTS AND SCOPE

The law does not specify that parties must meet and confer in the context of disclosure of ESI. There are provisions of law that relate to an obligation to produce evidence to a court in civil proceedings, which apply to all types of evidence.

Under the CPC, parties are obliged to produce evidence to establish facts to successfully argue their case. In this procedure, all parties might be obliged to submit, by order of the

2 By decision of the Warsaw Court of Appeal dated 24 October 2017, reference number: VII ACa 938/17.

3 By decision of the Łódź Court of Appeal dated 1 September 2016, reference number: I ACa 254/16.

court, on a specified date and in a specified place, the data in their possession that constitutes evidence of a fact relevant to the resolution of the dispute. There are no sanctions if a party refuses to produce the evidence requested, but the court may take this as an indication that the evidence contradicts the party's statement and therefore supports the opposing party's statement.

If a court requests a third party to produce evidence and it refuses to do so without legitimate grounds, it may be subject to a fine. If the third party does comply with the court's request, it has the right to demand reimbursement of expenses connected with producing the evidence.

V REVIEW AND PRODUCTION

Poland has only just begun to acknowledge the use of digital sources of information in statutes, such as the CPC and the Code of Criminal Procedure. Consequently, civil and criminal proceedings still tend to focus on traditional sources of evidence, such as paper documents, witness testimony and, in criminal cases, materials gathered by law enforcement authorities (the police and the public prosecutor) during operational activities, including lawful searches and interception of communications.

The limited regulation on the use of ESI covers the collection of ESI by law enforcement authorities during criminal proceedings; the obligation of parties to produce ESI as evidence; and the method of assessing ESI in civil proceedings.

According to Article 218a of the Code of Criminal Procedure, offices, institutions and companies conducting telecommunications activity are obliged, upon the request of the court or the public prosecutor in the form of a written decision, to immediately secure, for a period not exceeding 90 days, electronic data stored on data storage devices (e.g., hard drives) or in IT systems.

The Code of Criminal Procedure also provides that the holder and user of a device containing electronic data or an IT system has to acquiesce to a lawful search conducted by a competent authority with regard to the data stored on this device or in this system, or on a data storage device in their possession or use, including email correspondence.

A search is lawful under criminal law if there are justified grounds for believing that specified objects that might constitute evidence in a case or that are subject to seizure in criminal proceedings (e.g., electronic files) may be found on the premises (Article 219 Section 1). Objects that may serve as evidence or that are subject to seizure to secure financial penalties, penal measures of a financial nature, forfeiture, compensatory measures or claims for compensation for damage, should be surrendered at the request of the court, the public prosecutor or, in urgent cases, the police or another authorised agency (Article 217 Section 1). The holder of an object subject to seizure is called upon to surrender it voluntarily (Article 217 Section 2). However, if the holder refuses, the object may be seized by force, provided appropriate procedures are followed – for example, the holder should be properly informed about the legal basis for the seizure and a formal written protocol from the seizure should be drawn up (Article 217 Section 5).

A search may be conducted by the public prosecutor, acting upon an order of a court, or by the police, acting upon an order of a court or the public prosecutor, or, in cases specified by the law, by another agency (Article 220 Section 1). A person whose premises are to be searched should be presented with a warrant issued by a court or the public prosecutor

(Article 220 Section 2). In urgent cases, the authorities may conduct a search without the appropriate order, but approval from the court or public prosecutor must be sought promptly afterwards.

If the person on whose premises an object was seized or a search was conducted declares that a document found or surrendered contains confidential information, or information constituting a professional or other legally protected secret, or is of a private nature, the authority conducting the search should immediately, without reading it, hand the document over to the public prosecutor or to the court in a sealed envelope (Article 225 Section 1). However, the procedure does not apply to correspondence or other documents containing information classified as privileged or confidential, or information constituting a professional or other legally protected secret, if the holder is suspected of having committed an offence. It also does not apply to letters or other documents of a personal nature if the person suspected of having committed an offence is the holder, author or addressee (Article 225 Section 2).

Similarly, if the defence counsel declares that correspondence or other documents surrendered or found in the course of the search contain information pertaining to the performance of his or her function, the authority conducting the search must leave the documents with him or her without becoming familiar with their contents or appearance. However, if this statement is made by a person who is not a defence counsel, but is in possession of documents of that nature, the law requires the agency conducting the procedure to hand these documents over to the court, without reading them, in a sealed envelope. If the documents are seized, the court, having acquainted itself with their contents, must return them in their entirety or in part to the person from whom they were taken or must issue a decision that the documents be retained for the purposes of the proceedings (Article 225 Section 3).

The Code of Criminal Procedure also provides for general rules regarding interception of electronic communications. The rules that apply to the surveillance of telephone conversations also apply to the surveillance and recording by technical means of the content of other conversations or messages, including email correspondence (Article 241). The main rules are outlined below.

After the commencement of proceedings, the court, at the request of the public prosecutor, may order surveillance and recording of the content of telephone conversations by way of telephone tapping, to gather evidence for proceedings in progress or to prevent the perpetration of a new offence.

In urgent cases, surveillance and telephone tapping may be ordered by the public prosecutor, who is obliged to request the approval of the court within three days. The court must issue its decision on this matter within five days, at a closed hearing (without the participation of the parties). If the court does not approve the public prosecutor's order, any existing recordings must be destroyed. An appeal against the decision stays its execution.

Surveillance and telephone tapping are permissible with regard to a person suspected of an offence, an accused person, an aggrieved person or any other person whom the accused may contact or who may be connected with the accused or with the potential offence.

Offices and institutions conducting telecommunications activity, as well as telecommunications companies, are obliged to facilitate the execution of a court or public prosecutor's order concerning surveillance and telephone tapping, and ensure that they register the surveillance.

With regard to civil procedure, the regulations are more general. In practice, any advanced analytical tools involved in the analysis, review and production of ESI are most likely to be used by expert witnesses requested by the court or parties to participate in a given proceeding.

The Polish legal system is based on the idea that the courts are free in their assessment of the impact and admissibility of evidence presented during the proceedings. As a consequence, no precise rules regarding the use of technology-assisted review or the manner in which ESI should be collected or secured have been adopted in the procedural codes of Polish law. The courts generally rely on the testimony of expert witnesses who – when summoned by the court – have to assess certain aspects of the evidence, as requested by the court.

In both civil and criminal proceedings, the party against whom electronic evidence is presented may challenge the evidence by raising arguments about its value, authenticity, admissibility or quality. In doing so, the party may also request to consult an expert witness, which is the most reasonable way to have the evidence verified. Ultimately, it is up to the court to decide whether those arguments should prevail and if the evidence should be disqualified. The law does not provide sanctions for failure to produce discoverable ESI or misuse of disclosed ESI. Only general rules apply, according to which, if so directed by the court, each party shall produce, within a prescribed time limit and at a specified place, any document that is in its possession and that evidences a fact that is relevant to the case determination, unless the document contains classified information (Article 248 Section 1). As mentioned in Section IV, if a third party refuses to produce evidence, it will be fined by the court if it, or the parties, cannot justify the refusal (Article 251).

VI PRIVACY ISSUES

On 25 May 2018, the General Data Protection Regulation (GDPR) entered into force and became directly applicable in Poland and the other Member States of the European Union. The GDPR has a significant impact on the discovery and disclosure of ESI, whenever this information (wholly or even partly) relates to an identified or identifiable natural person. In such cases, the rules for processing personal data set out in the GDPR apply and must be observed by any person or entity that determines (alone or jointly with others) the purposes and means of the processing of personal data (i.e., the data controller).

A particularly significant issue related to personal data processing is the necessity to identify a valid legal basis for processing activities, such as storing (including in electronic form) and sharing (granting access to) personal data. In accordance with Article 6.1 of the GDPR, processing shall be lawful only if and to the extent that at least one of the following applies:

a the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b processing is necessary for the performance of a contract to which the data subject is party or to take steps at the request of the data subject prior to entering into a contract;

c processing is necessary for compliance with a legal obligation to which the controller is subject;

d processing is necessary to protect the vital interests of the data subject or of another natural person;

e 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 controller; or

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

The defined catalogue of legal bases for personal data processing requires data controllers, in circumstances regarding discovery or disclosure of ESI comprising personal data, to search for and choose an applicable option. Generally, in court proceedings, the reasons set out in points (c) and (f), above, are applicable.

The reason in point (c) may be relied upon by the data controller if a specific provision of law requires a person or entity to disclose certain categories of personally identifiable information for a specific purpose. Under Polish law, an example of this is a list of required information to be included in admissible pleadings (Article 126 of the CPC). However, owing to the versatile nature of potential evidence in both criminal and civil cases, it seems unlikely that a provision of law will be sufficiently precise as to the scope and purpose of personal data to be disclosed for a controller to be able to rely upon it.

Consequently, the reason in point (f) must be considered by a controller wishing (or required to) disclose personal data or obtain it in the course of (or in relation to) legal proceedings. The existence of a legitimate interest of a controller (or a third party) needs to be assessed, taking into account various factors. Recital 47 of the GDPR indicates that the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. The Recital specifies that the existence of a legitimate interest would need careful assessment, including of whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. Because of that, the controller – when collecting personal data – must be diligent when editing its data processing information clauses, required by the GDPR, and ensure that the potential disclosure of personal data within relevant proceedings is listed as a potential form of processing of an individual's data. The Recital goes further to indicate that interests and fundamental rights of the data subject could override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

According to the GDPR, processing of personal data strictly necessary for the purposes of preventing fraud constitutes a legitimate interest of the data controller concerned. In any case, a particular disclosure will require the controller to perform a legitimate interest test and, according to its outcome, disclose or refrain from disclosing the data, at least in a form that identifies the data subject.

Another issue is that, should a controller decide to anonymise the data it is submitting in proceedings, the information could be dismissed by the court as altered and not admissible as evidence.

The GDPR also includes a separate list of circumstances allowing for lawful processing of certain categories of personal data, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for the purpose of uniquely identifying a natural person), data concerning health,

or data concerning a natural person's sex life or sexual orientation. One of the admissible circumstances is when processing is necessary for the establishment, exercise or defence of legal claims (Article 9.2(f)).

As an EU Regulation, the GDPR does not restrict transfers of data within the European Union. However, transferring personal data outside the European Union (or, more specifically, the European Economic Area (EEA)) is restricted, unless specific conditions are met. These conditions depend on the level of risk posed by different circumstances accompanying a given transfer. Therefore, a transfer of personal data to a third country or an international organisation may take place if the European Commission (the Commission) has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. This type of transfer does not require specific authorisation (Article 45 of the GDPR).

In the absence of an adequacy decision from the Commission, a controller may transfer personal data to a third country or an international organisation only if it has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available (Article 46.1). The appropriate safeguards may constitute:

a a legally binding and enforceable instrument between public authorities or bodies;
b binding corporate rules (within a group of companies);
c standard data protection clauses adopted by the Commission in accordance with the examination procedure;
d standard data protection clauses adopted by a supervisory authority and approved by the Commission pursuant to the examination procedure;
e an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
f an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

If there is no adequacy decision from the Commission, nor any appropriate safeguards in place, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only under strict conditions, one of which is that the transfer is necessary for the establishment, exercise or defence of legal claims (Article 49.1(e) of the GDPR). This circumstance, however, must be sufficiently justified and documented by the transferor.

According to Article 48 of the GDPR, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the European Union or a Member State, without prejudice to the other admissible grounds for transfer, described above.

VII OUTLOOK AND CONCLUSIONS

Providers of e-discovery services in relation to pre-litigation and litigation matters are becoming increasingly common. As demand for these services is clearly growing, it is likely to be a hot topic in Poland in 2019. Consequently, we feel that the Polish legislature should review the legal framework with a view to updating it by incorporating provisions on the collection and use of ESI. This would be beneficial for parties to proceedings, lawyers and the courts.

Chapter 10

SPAIN

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

I OVERVIEW

As opposed to 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 breach, 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' or 'documents', which are most commonly used by the legislature.

---

1 Enrique Rodríguez Celada is a 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 (1) to obtain a medical file, (2) to determine the members of a group of consumers or users affected by a certain product, or (3) 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.

Finally, as a result of having no discovery process, the 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 in other jurisdictions. However, this has started to change, as expansive information requests, new technologies and internal investigations are becoming more commonplace (see Section V).

II YEAR IN REVIEW

The laws that refer to data preservation and disclosure obligations, especially the former, are in constant development and consequently so are the provisions.

For example, the amendment to the Anti-Money Laundering and Terrorist Financing Law of 28 April (Law 10/2010) by Decree-Law 11/2018 of 31 August broadened the scope of legal and natural persons obliged to comply with its provisions (including data preservation obligations). As a result, online gambling providers are now obligated to preserve data as established in the amended Article 2.1.u (in addition to other individuals and legal entities already subject to the anti-money laundering obligations, such as credit institutions, investment firms, audit firms, accounting companies and tax advisers). The amendment has also altered the wording of Article 2.1.o, which now refers 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. Nevertheless, the practical consequences of this amendment (the introduction of the clause 'on behalf of a third party') remain unclear and have yet to be determined by administrative authorities or case law.

Although the period to preserve relevant documents is still 10 years, there is now an obligation to destroy all documents after this period. The amendment has also limited the individuals or entities entitled to access the preserved documents after the first five years to only the corporate organisms in charge of internal control within the company.

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 the 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 the legal entity as a whole, and not on specific natural persons within it.

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 activity, 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 that Law's anti-money laundering obligations. As a result, this preservation responsibility extends to:

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

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

c all documents supporting the actual implementation of internal controls with regard to a client and the communications made to the anti-money laundering authorities regarding a client or transactions with the 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).

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

Stock market regulations (primarily the Market Abuse Regulation[3] and the Spanish Stock Market Law[4]) create additional obligations involving the preservation of all documents related to market soundings[5] (including any correspondence and recording of these communications) and insider lists[6] for five years.

The banking and financial field is also subject to numerous preservation obligations. The Stock Market Law requires that entities that participate in the securities and investment market perform and store suitability tests to corroborate the fitness of a specific client to invest in a particular product (and 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 these entities (Circular 5/2017 of 27 June).

As a final example, telecommunication companies are also obligated 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 the event that the records contain personal data as defined by the EU General Data Protection Regulation (GDPR),[7] this personal data must be erased

3 Regulation (EU) No. 596/2014.

4 Law 4/2015 of 23 October.

5 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'.

6 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'.

7 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

when no longer necessary for the legitimate purposes for which it was obtained or processed, 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 the processing, and only for the time during which the liability may arise). When the liability expires, the data must be deleted. Therefore, 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 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 this data is issued (as explained in Section IV).

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, the 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 of 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 the counterparty disclose documents. Despite establishing a highly generic obligation to provide information in judicial proceedings (as per the request of a counterparty), this Article nevertheless limits the scope of the party's request to documents that (1) are not available to the requesting party and (2) 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 Spanish jurisdiction). In addition, according to Article 328.2 of the Civil Procedural Law, the requesting party has to 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 the 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).[8] The amended regulation aims to broaden access to evidence within these cases by setting out a process to request the disclosure of data. However, this new process still requires the intervention

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'.

8 This regulation amended the Civil Procedural Law pursuant to, among others, 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.

of a court to issue the judicial order to gather the relevant documents and information. In addition, the new regulation on these specific proceedings does not permit a general request of information similar to discovery. In fact, the party's request has to meet different requirements that may limit the scope of the data demanded. In this regard, at the moment of issuing the judicial order, the court has to 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 is 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. Furthermore, the requesting party will have to bear the costs of obtaining the evidence, which are quantified on a case-by-case basis. For this purpose, the court can order the 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[9]). 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;[10] this approach is also subject to limits set forth by the Criminal Procedural Law (Articles 545 to 578), with the most notable limitations being the prohibition to carry out futile inspections or seize documents that are not deemed necessary for the investigation of the 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 Articles mentioned above, the 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 will be drafted describing how the raid was carried out and listing the documentation that was seized.

9 As opposed to other jurisdictions, in Spain, the payment of 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 these 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.

10 According to Spanish law, a court can also order in a same writ a request of 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.

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.[11] Within the amended legislation, Article 588 *sexies* (a) to (c) addresses the inspection of ESI. According to these 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 the 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 these articles, the scope of the seizure can be broadened during the course of the 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 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 the seized devices, provided that this inspection is essential and that they communicate the circumstance 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 the 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.

With respect to 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 these, the Criminal Code sanctions procedural fraud, which consists of 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 consists of 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).

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

Nevertheless, Spanish case law has clarified that 'mere concealment of information' is not criminal,[12] even when the concealed information is 'relevant', as this omission cannot be equal to actually deliberately misleading the Court.[13] Therefore, this criminal offence, as interpreted by the courts, does not result in a general obligation to preserve and disclose data.

It is also a criminal act to conceal, alter or disable the *corpus delicti*, the outcome of the offence or the instruments used to commit it, with the purpose of impeding the discovery of the criminal offence (Article 451(2)). According to Spanish case law, these concealing actions are sanctioned when carried out (1) knowing (and not only suspecting or assuming) the existence of the offence that is sought to be concealed; (2) by someone who has not been involved in the commission of the concealed offence; and (3) provided that the action of concealing is performed after the perpetration of the concealed offence.[14] The sentence of imprisonment to be imposed in these cases ranges from six months to three years.

Finally, the Criminal Code also punishes disobedience toward authorities (Article 556), provided that:

a the order challenged is final, direct and explicit, and imposes on the 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 that the authority should previously warn the individual about the potential criminal consequences of his or her actions, although it is common practice to give notice to the concerned 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.

Therefore, 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 the specific case). In fact, court orders reiterating a prior judicial order (e.g., a request to disclose specific documentation) frequently warn the corresponding party of their potential criminal liability for the commission of the 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 consisting of failure to disclose the company's accounting files.[15] 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.

12 Ruling 366/2012, of 3 May, of the Criminal Section of the Supreme Court.
13 Ruling 1899/2002, of 18 November, of the Criminal Section of the Supreme Court.
14 Ruling 178/2006, of 16 February, of the Criminal Section of the Supreme Court.
15 Ruling 136/20, of 18 February.

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

As explained in Section I, 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.

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 the criminal file for analysis by the court and the parties to the 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 these kinds of situations, lawyers tend to involve a forensics company to ensure proper preservation and review of the data. However, law firms are still in charge of directing the investigation and making the strategic decisions, and the intervention of an attorney remains necessary for the investigation to be subject to legal privilege. These forensics companies have implemented some of the international techniques for the analysis of information (e.g., software tools to carry out key-word searches and corporate intelligence resources). However, use of predictive coding and email threads is not yet widespread.

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 thus far) has traditionally implied that legal privilege is not as frequently challenged in Spain as 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 gaining more importance.

Notwithstanding these potential future changes, the current situation regarding legal privilege is as follows: the right to claim privilege is acknowledged by Article 5 of the Code of Conduct for Spanish Lawyers, together with Article 32.1 of the Lawyers' General Statute and Article 524.3 of the Basic Law on the Judiciary. The scope of this privilege extends to:

a all facts known by a lawyer from a client as a result of his or her involvement in providing legal advice (Article 5.1);

b any confidential information or proposal received by the lawyer from the client, counterparties in the case and other professional colleagues, as well as any data or document received by the lawyer as a result of his or her professional activity (Article 5.2); and

c any communication exchanged between the lawyer and his or her client, or with the counterparties or their lawyers, which, in addition, cannot be recorded unless previously consented to by all participants (Article 5.4).

The law does not expressly refer to the work-product doctrine, although it is generally accepted that the protection of legal privilege also extends to these documents, which involve the relaying of facts by the client and legal advice on the matter.

With regard to the exceptions to legal privilege, there are some particularities affecting in-house lawyers, lawyers advising on transactions that are subject to Law 10/2010 and tax advisers.

The extension of legal privilege to in-house lawyers remains a matter of debate as Spanish legislation and European rulings are not entirely aligned. According to the Court of Justice,[16] in-house lawyers and external lawyers have distinct situations given the hierarchical integration of the former within the company that employs him or her. 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, none of the Spanish regulations previously referred to makes a distinction between the two types of lawyers. On these grounds, the Administrative Section of the Supreme Court has stated that confidential documents exchanged between an in-house lawyer and his or her company are also subject to legal professional privilege pursuant to the same conditions applicable to external lawyers' communications.[17] Notwithstanding this, the Supreme Court does limit legal professional privilege and considers that this has not been infringed when the documents or correspondence exchanged between the lawyer and the client that are disclosed do not affect the lawyer's right to defend the client (i.e., when the disclosure of this information has no impact on the client's exercise of his or her right to defence). In any case, in practice, the European Commission's approach to this matter is also taken into consideration by Spanish lawyers and Spanish case law is expected to develop in this field.

As regards exceptions to legal privilege foreseen by anti-money laundering regulations, Law 10/2010 includes attorneys as professionals subject to the anti-money laundering obligations whenever they participate in the design or performance of, or provide advice on behalf of a client in, the sale of real estate or commercial entities; the management of funds, stocks or other assets; the opening and management of bank accounts or stock accounts; the setting up, functioning or management of companies or trusts, or similar entities; or whenever they act on behalf of a client in any financial or real-estate transaction.[18] However, Article 22 of the same Law excludes lawyers from the obligation to report and cooperate with the authorities regarding the information they receive from their clients for the determination of their legal situation once the transaction has been carried out, or for their defence in judicial proceedings. According to the guidelines set forth by the General Council of Spanish Lawyers, the lawyer's

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

17 Ruling 337/2018, of 12 February.

18 Article 2.1(n), Law 10/2010.

advice will be subject to legal privilege when it is provided after the suspicious transaction has been performed, but the advice will not be subject to legal privilege if it takes place before the execution of the transaction and for the purpose of carrying this out.

Finally, legal tax advisers may also face challenges in future years as the ongoing amendments to the General Tax Law could limit the legal professional privilege of these lawyers. The purpose of the amendment is to incorporate the content of Directive (EU) 2018/22 of 25 May, on mandatory automatic exchange of information in the field of taxation in relation to reportable cross-border arrangements into Spanish legislation. This Directive expressly criticises the apparent contribution of intermediaries and tax advisers to their clients' concealment of funds abroad and requests that EU Member States pass the necessary laws to ensure that intermediaries report any cross-border transactions to the competent tax authorities that are deemed reportable in accordance with applicable EU and national tax legislation. The question of legal privilege now relies on whether the amended Spanish legislation will include legal advisers among these 'intermediaries' and if, as a result, communications exchanged between them and their clients would no longer benefit from legal privilege and could be requested in the context of judicial proceedings that could be initiated in the context of an investigation of a cross-border transaction. As the amendment to the Spanish legislation remains in the initial stage (the proposal has not yet been published), it is far too soon to anticipate what the final wording of the General Tax Law will be, or its practical consequences.

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 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 these 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 (and, if the information in question is sensitive personal data, a ground for processing under Article 9 of the GDPR must also exist).

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 the 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 this Article must be laid down by the EU law or Member State law to which the controller is subject. Therefore, e-discovery and any enforcement requests based on these laws require a complex case-by-case analysis from a data protection standpoint.

In addition, personal data transfers to countries that do not ensure an equivalent level of protection are permitted only if the controller or processor has provided appropriate safeguards, 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 the Guidelines 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 the 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 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 the data exporter to institute procedures in a third country (e.g., commencing litigation, seeking approval for a merger). Notwithstanding this, the derogation cannot be used to justify the transfer of personal data on the grounds of the mere possibility that legal proceedings or formal procedures may be brought in the future.

In addition to the above, 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).

Finally, the disclosure of personal data would require providing prior notice of the possibility of personal data being transferred to and processed by foreign authorities. If the 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 and 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 the 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 coming years.

Chapter 11

UNITED STATES

Jennifer Mott Williams[1]

I OVERVIEW

The law governing electronic discovery (e-discovery) is continually developing. US courts, administrative agencies and regulatory bodies often have an expansive view of discovery of electronically stored information (ESI). This view stems from the notion that broad discovery helps facilitate the quest for truth.

The Federal Rules of Civil Procedure (the Federal Rules), state procedural rules, the Federal Rules of Evidence, state evidentiary rules, regulatory agency rules, other local rules, and case law created by judicial and regulatory opinions, have created a patchwork of law governing e-discovery. Although courts and regulatory authorities are adapting evidentiary and procedural rules to the realities of e-discovery, courts, regulatory authorities and litigants have struggled to keep up with ever-changing technologies and data proliferation. The Federal Rules intentionally avoid defining the term 'electronically stored information' with precision in order to accommodate '[t]he wide variety of computer systems currently in use, and the rapidity of technological change'.[2] Thus, the Rules envision the discovery of 'any type of information that is stored electronically',[3] including forms of ESI not yet invented.

In the United States, the producing party typically bears the costs of producing ESI. For years, litigants struggled with increasing e-discovery costs. Explosions in data volumes coupled with expansive views of discovery resulted in e-discovery costs that threatened to overwhelm litigation. Moreover, courts took varying approaches in sanctioning parties that failed to preserve ESI – some courts granted adverse inferences that, in essence, determined the outcome of a matter when parties were deemed negligent or grossly negligent in failing to preserve ESI, while others only granted these sanctions when a party acted in bad faith to deprive the opposition of evidence. Litigants grew increasingly concerned that cases were being decided based upon the costs of discovery and threat of sanctions as opposed to the merits.

Recognising the need to rein in e-discovery costs and provide more uniformity and certainty for litigants, the Federal Rules were amended in December 2015 to explicitly make proportionality an element of the scope of discovery and to reserve outcome-determinative sanctions for those cases where a party acts in bad faith.

---

1 Jennifer Mott Williams is an associate at Morgan, Lewis & Bockius LLP.

2 Fed. R. Civ. P. 34 advisory committee's note (2006).

3 ibid.

Generally, the scope of discovery is governed by Rule 26(b)(1), which allows a party to discover:

> *[A]ny nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.*

Moreover, for years, parties were at odds with one another when it came to e-discovery. Despite the contentious nature of US litigation, courts and litigants are recognising the need for parties to work together to bring about the 'just, speedy, and inexpensive'[4] determination of a matter. Thus, the Federal Rules and local rules have been amended to improve cooperation between parties through requiring meet and confers, and informal e-discovery discussions.

A party can help control its e-discovery costs as well as the entire e-discovery process through thoughtful, strategic planning, knowledge of the ESI landscape and understanding the needs of the case. Armed with this knowledge, responding parties may lessen the burdens placed upon them and might even seek to shift costs when requested data is thought to be inaccessible or seems to be duplicative of previously produced information, or when the costs associated with production are in excess of an amount thought to be reasonable and proportional.

II YEAR IN REVIEW

With the December 2015 amendments to the Federal Rules and related changes in e-discovery laws, litigation is more likely to be decided on the merits. The imposition of the harshest outcome-determinative sanctions has been dramatically reduced, with courts imposing harsh sanctions under Rule 37(e) only in those instances where there has been an intent to deprive. Increasingly, courts, regulatory authorities and parties are invoking proportionality when viewing preservation and production obligations, narrowing e-discovery to those areas of enquiry necessary to resolve a claim.

Courts continue to seek new ways to reduce the time and costs associated with e-discovery. The District of Arizona and the Northern District of Illinois are midway through the Mandatory Initial Discovery Pilot Project, which requires parties to respond to standard discovery requests before undertaking other discovery.

New rules and regulations on the horizon require parties to cooperate. Proposed Federal Rules amendments require that parties meet and confer before any 30(b)(6) deposition, which may be of particular importance when faced with the proverbial 'discovery about discovery' deposition, seeking testimony about how data was preserved, collected and produced. In addition, more and more courts are instituting local rules requiring meet and confers before e-discovery issues are raised with courts.

Courts and parties must remain efficient in addressing the ever-changing landscape of e-discovery and technology itself. Because ESI subject to discovery encompasses information in any form, recent cases in the past few years have focused on newer technologies, including cloud computing, mobile devices and communication applications. Aside from general

4 Fed. R. Civ. P. 1.

information governance and privacy concerns, as well as issues with trying to collect and produce this information, use of newer technologies, such as cloud file shares, can expose a party to the risk of waiving privilege.

While the laws governing e-discovery continue to evolve, there are still issues that must be resolved.

i State rules versus the Federal Rules

Although the Federal Rules were amended in 2015 to try to address proportionality and sanctions concerns, not all states have accordingly updated their respective rules. Therefore, parties may still face uncertainty with respect to discovery in state court litigation.

ii Redactions for irrelevant information

Some courts allow parties to redact non-responsive information, while others reject this practice.[5] Courts denying redactions cite the lack of authority for them and the need for a party to see information in context, while courts allowing redactions often find compelling reasons for them, such as protecting unique business information, and believe that requesting parties are not entitled to irrelevant information.

iii Quick peeks

Courts appear to disagree on the scope and meaning of Federal Rule of Evidence 502 and its interplay with Rule 26. When faced with burden and proportionality arguments, some courts are requiring parties to provide a 'quick peek' under Rule 502(d), allowing the opposing party to view all documents without the producing party risking privilege waiver.[6]

iv Extraterritorial discovery

Cross-border discovery remains a moving target. In March 2018, Congress passed, and President Trump signed, the Clarifying Lawful Overseas Use of Data Act (the CLOUD Act). The CLOUD Act has made clear that Stored Communications Act Section 2703 warrants apply to data held outside the United States. The CLOUD Act requires a company with US contacts to preserve and disclose the contents of a stored communication 'regardless of whether such communication, record or other information is located within or outside of the United States'.[7] However, the CLOUD Act does contain comity provisions that may limit the US government's ability to access data stored abroad, including where the target customer is not a US person and does not reside in the US or where disclosure of the data would violate foreign law. Owing to the CLOUD Act's passage and issuance of a new subpoena thereunder, the highly publicised United States Supreme Court case *United States v. Microsoft*, dealing with issuance of a warrant seeking data stored overseas in Ireland, was dismissed as moot in a *per curiam* opinion.

---

5 Compare *IDC Financial Publications, Inc. v. Bonddesk Group, LLC*, No. 15-cv-1085-pp, 2017 WL 4863202 (E.D. Wis. Oct. 26, 2017), with *In re Takata Airbag Products Liability Litigation*, 14-24009-CV-MORENO, 2016 WL 1460143 (S.D. Fla. Feb. 24, 2016).

6 See, e.g., *Fairholme Funds, Inc. v. United States*, 134 Fed. Cl. 680 (Fed. Cl. 2017). Others have rejected this reasoning, noting that the scope of discovery is governed by Rule 26(b), which explicitly excludes privileged information. See *Winfield v. City of N.Y.*, 15-cv-05236, 2018 WL 2148435 (S.D.N.Y. May 10, 2018).

7 CLOUD Act Section 103(a)(1).

Lower courts remain divided on the production of documents located outside the United States. Some courts are trying to remove data subject to foreign data regulations from the discovery process as much as possible.[8] Others are applying proportionality concepts in determining whether foreign data is really relevant or can be narrowed in some manner,[9] and still others are ordering extraterritorial discovery under other rules, such as 28 USC Section 1782.[10]

III CONTROL AND PRESERVATION

i The duty to preserve ESI

Generally, the duty to preserve arises whenever there is a reasonable anticipation of litigation. Reasonable anticipation of litigation includes not only traditional litigation filed by one party against another, but also any proceedings before administrative agencies or other regulatory bodies.

ii The scope of preservation

The general scope of discovery – which encompasses anything relevant and proportional to the needs of the case – governs the scope of preservation. Thus, whenever the duty to preserve arises, a party must take affirmative steps to identify and preserve unique, potentially relevant and proportional ESI in the party's possession, custody or control.

Preservation extends beyond the ESI within a party's physical possession to that over which the party has the 'legal right' to obtain the ESI upon demand. This legal right may be found when there are contractual provisions granting a right of access to ESI or when there is a principal–agent relationship that provides the principal with ownership of data in the agent's possession, such as the relationship between an employer and an employee, a client and an attorney, or a corporation and an officer or director. Furthermore, some jurisdictions expand the concept by finding that ESI is under a party's control when the party has the practical ability to obtain the ESI from a non-party, such as when a party could likely ask for the documents and obtain them from the non-party. Thus, parties may need to look to third parties for potential document preservation, including cloud storage providers, administrators of computer systems, payroll vendors, and individual employees or agents storing data on personal phones or home computers.

iii Limitations on the duty to preserve

Though very broad, preservation is not limitless. Parties are not required to preserve every piece of ESI. Preservation efforts should be proportional to the needs of the case 'considering

8 See Ex. B. to N.Y. Commercial Division Part 53 Practice Rule (providing that data subject to the EU General Data Protection Regulation or other foreign laws restricting the processing or transfer of data to the United States need not be searched and produced).

9 See *In re Bard IVC Filters Products Liability Litigation*, 317 F.R.D. 562 (D. Ariz. 2016); and *In re Davol, Inc./C.R. Bard, Inc. Polypropylene Hernia Mesh Products Liability Litigation*, 2019 WL 341909 (S.D. Ohio Jan. 28, 2019).

10 See *In re Accent Delight International Ltd.*, 16-MC-125, 2018 WL 2849724 (S.D.N.Y. June 11, 2018), appeal filed (rejecting claim that Section 1782 only permits discovery of information located in the United States in ordering production of information from offices of a foreign affiliate because Section 1782 allows a court to order any person who 'resides or is found' in the district to produce documents).

the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit'.[11] ESI that has marginal utility or relevance is more likely to be found disproportional for purposes of preservation.

Unfortunately, proportionality can be an amorphous standard that can be difficult to apply, which means that parties faced with costly preservation efforts should seek to negotiate preservation obligations with opposing parties. If agreement cannot be reached, parties may be forced to seek court intervention, at which time they must be prepared to explain the specific burden or cost associated with preserving material along with why the information is of little benefit.

iv Penalties for failure to preserve ESI

If a party fails to preserve ESI in anticipation of litigation, Rule 37(e) governs the sanctions available. The Rule 'forecloses reliance on inherent authority or state law to determine when certain measures should be used'.[12] Under this Rule, sanctions will only apply if a party had a duty to preserve information and failed to take reasonable steps to preserve; the information was lost because the party failed to take reasonable steps; the information could not be restored or replaced through additional discovery; and the loss of the information was prejudicial.

Assuming all criteria for sanctions have been met, any sanction granted must be no greater than necessary to cure the prejudice created from the loss. The determination of an appropriate sanction is left to the sound discretion of the judge and should be assessed on a case-by-case basis. Sanctions for failure to preserve may vary, and can include an award of attorney's fees, cost shifting, evidentiary restrictions, issue preclusion, striking claims and defences, special jury instructions, and default judgment or dismissal. However, Rule 37(e) imposes a uniform standard for the use of more severe sanctions, such as adverse inferences, dismissal or default judgment, limiting the most severe sanctions to only those instances when a party intentionally destroyed information with an intent to deprive another party from using the information in the litigation. Courts may not circumvent this standard by granting a 'lesser' sanction that would have the same effect as the harsher sanctions permitted only when there has been an intent to deprive, such as granting evidentiary restrictions that preclude a party from offering any evidence or striking an entire pleading so that the party no longer has claims or defences.

IV REQUESTS AND SCOPE

i Rule 26(f) – meet and confer

Rule 26(f) requires that parties meet and confer to discuss issues related to preserving discoverable ESI as well as to develop a discovery plan that will govern collection and production of ESI. This meet and confer provides litigants with an opportunity to control the discovery process and rein in discovery costs.

11 Fed. R. Civ. P. 26(b)(1).

12 Fed. R. Civ. P. 37 advisory committee's note (2015).

Among other items, the required discovery plan must include:

a the subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues;

b any issues about disclosure, discovery or preservation of ESI, including the form or forms in which it should be produced;

c any issues about claims of privilege or protection, including whether to ask for an order under Federal Rule of Evidence 502 to protect against waiver of privilege by production; and

d what changes should be made in the limitations on discovery imposed by the Federal Rules or local rules as well as what other limitations should be imposed.

Parties should be prepared to discuss the topics about which discovery will be sought; custodians from whom discovery will be sought; non-custodial sources of data from which discovery will be sought; inaccessible data; the preservation process and any limitation on preservation; the relevant time frame for ESI; methods for searching for relevant ESI; the format in which ESI should be produced; protection of confidential information or trade secrets; issues related to data located outside the United States; 502 privilege protections; and any proposed staging or limiting of discovery.

ii Making Rule 34 requests for production

Using the discovery plan as a framework, a litigant may request that the opposing party produce ESI within its possession, custody or control that is relevant to any party's claims or defences and proportional to the needs of the case, not just those that it may use to support its own claims or defences.

Requesting parties are obligated to seek ESI that is relevant and proportional to the needs of the case. Requests for ESI must be reasonably specific, as requests for 'any and all' emails or other ESI are typically disfavoured by courts and deemed disproportional to the needs of the case.

If the discovery plan has not adopted a production format for ESI, the discovery requests should also specify the form or forms in which different types of ESI should be produced.

iii Responding to Rule 34 requests for production

When responding to discovery requests, a party must either object to the requests or produce any responsive, non-privileged ESI within its possession, custody or control that has been requested. In determining whether to object, responding parties will need to assess whether the request seeks relevant and proportional information within its possession, custody or control in the format agreed to by the parties. If not, responding parties should object.

Objections and responses to requests should be specific, state whether the responding party is withholding any responsive documents on the basis of an objection, indicate whether the responding party is producing copies of documents or ESI, or instead is permitting inspection of the documents or ESI, and state whether the production or inspection will be made by the time specified in the request or at another reasonable time specified by the producing party. 'Boilerplate objections' or lists of very general objections made at the beginning of the responses are not allowed and are considered meaningless.

Some objections are unique to ESI requests. For example, a party should object if the other side seeks direct access and inspection of the party's computer systems. Direct access

to a party's electronic systems is typically not permitted without a finding of some sort of discovery misconduct or the presence of unique factual circumstances that might necessitate access, such as when theft or misappropriation of trade secret data has been alleged. A party should also object when the opposing party seeks inaccessible ESI, such as data that requires restoration or forensic recovery. Whenever lodging an inaccessibility objection, the party must identify the data that is not being searched and produced. Similarly, another unique ESI objection is an objection to the format of production requested. If a responding party objects to the requested form of production, the responding party must state the form in which it intends to produce ESI. This form must be either the form in which the ESI is ordinarily maintained or a reasonably usable form.

More general objections that apply to all discovery can take on further importance when ESI is implicated. A responding party should object to any request that is disproportional to the needs of the case when the information sought is of marginal utility to resolving the issues. When lodging a proportionality objection, the responding party must be prepared both to quantify the costs associated with collecting and producing the ESI and to demonstrate the ESI's lack of usefulness to the litigation. Another common objection is that requests are overly broad, such as when they seek 'all' of a type of data, or are not reasonably limited in time frame or the number of sources to be searched. Given the proliferation and redundancy of data, a responding party should object to a request seeking ESI that is cumulative or duplicative of ESI already produced, or that might be obtained from another more convenient source.

iv Rule 45 subpoenas

ESI may also be sought by subpoena from a third party, though like discovery from parties, the breadth and scope of discovery from non-parties is limited by the relevance and proportionality requirements of Rule 26. Courts often find that third parties should be afforded more proportionality protections. Parties issuing subpoenas are required to take steps to minimise the burden on third parties and protect third parties from undue expense.

As with parties responding to discovery requests, a third party responding to a subpoena has a duty to preserve relevant data and may object to requests seeking data that is disproportionate to the needs of the case or that is not reasonably accessible. The party responding to a subpoena has the burden of demonstrating any burden associated with the subpoena and why the subpoena should be modified or quashed.

V REVIEW AND PRODUCTION

i ESI production timing

Parties are required to make initial disclosures within 14 days of the parties' Rule 26(f) conference. The initial disclosures must describe or provide copies of ESI that the disclosing party 'may use to support its claims or defenses'.[13]

Parties are further required to respond to Rule 34 requests for production within 30 days of being served or within 30 days of the Rule 26(f) conference, if served beforehand. In practice, parties will provide their written objections to requests and written responses within 30 days. However, the actual production of documents may come much later. The Federal Rules require that production be completed 'no later than the time for inspection

13 Fed. R. Civ. P. 26(a)(1)(A)(ii).

specified in the request or another reasonable time specified in the response'.[14] Given the time often necessary to collect and review ESI, responding parties may negotiate timelines for production with opposing parties. Alternatively, absent an ability to agree, responding parties may specify a time to begin making productions and may continue to make supplemental 'rolling' productions of documents until review is completed.

ii Review tools

There are many tools litigants may use to analyse data to determine what must be produced, including objective filtering (such as filtering by date), term and phrase searching, domain analysis, message threading, near-duplicate identification, concept clustering and visualisation tools. In addition, many US litigants employ technology-assisted review (TAR), which refers to machine-assisted classifying technologies, to facilitate review and analysis.

The rationale for using any analytic tool, and particularly TAR, is to reduce the cost of review by assisting individuals in identifying the documents most likely to be responsive while helping individuals separate out and avoid reviewing non-responsive documents.

US courts are increasingly encouraging the use of TAR to promote the aims of Rule 1 – a just, speedy and inexpensive determination of the action. Yet, courts have been reluctant to require the use of TAR thus far, deeming the producing party to be in the best position to determine how to search for, review and produce responsive ESI.

While many litigants have embraced TAR, technologies are constantly evolving, with new review technologies on the horizon. Artificial intelligence (AI) technologies are being developed to assist in analysing data for US litigation. Ultimately, no matter what technology is chosen, a litigant must be able to explain any technology used, old or new, and how that technology produced defensible results.

iii Protecting privileged ESI in e-discovery

Parties need only produce non-privileged, responsive ESI to another party. As such, privileged documents, including those protected by attorney–client privilege and work-product immunity, need not be produced. Technological tools may be employed to assist attorneys in locating privileged documents requiring protection from disclosure.

Whenever ESI is withheld because of an applicable privilege, the party must 'describe the nature of the documents, communications, or tangible things not produced or disclosed – and do so in a manner that, without revealing information itself privileged or protected, will enable the other parties to assess the claim'.[15] This Rule has led to parties creating logs of privileged documents being withheld. The contents of these logs may be the subject of local rules and can also be the subject of an agreement between the parties.

Yet, even when technological tools are employed and documents have been logged, the vast quantity of ESI poses significant challenges when trying to protect privileged information from being disclosed. For years, courts embarked on varied analyses to determine whether the disclosure of privileged ESI through mistaken production constituted a privilege waiver. Now, parties may avoid these varied analyses altogether by seeking an order under Federal Rule of Evidence 502(d) to protect against the waiver of attorney–client privilege or work-product immunity by the mere production of ESI. This order can protect a party from incurring

14 Fed. R. Civ. P. 34.

15 Fed. R. Civ. P. 26(b)(5).

protracted arguments over whether a privilege has been waived under the default Federal Rule of Evidence 502(b) standard, including arguments over whether the disclosure was inadvertent, whether the holder of the privilege took reasonable steps to prevent disclosure and whether the holder of the privilege took reasonable steps to rectify the disclosure.

iv Challenging an opponent's production

If a party believes an opponent's production is incomplete, the party should raise the issue with the opponent. Should the parties be unable to resolve the issue, the requesting party may file a motion to compel production under Rule 37(a). Failure to meet and confer before filing the motion to compel will preclude the moving party from seeking costs for making the motion.

Other mechanisms for challenging a production can be found in Rule 37. If the court has entered a discovery order and the opponent fails to comply, the requesting party should file a motion under Rule 37(b). A requesting party might file a motion under Rule 37(c) if its opponent fails to supplement responses and provide information requested in discovery. Under Rule 37(d), a requesting party may seek sanctions if its opponent wholly fails to serve its answers, objections or written responses to a request for production.

VI PRIVACY ISSUES

A business within the United States is generally required to preserve, collect and produce data within the organisation's possession, custody or control. Unlike in other jurisdictions throughout the world, where an employee or data subject about whom information relates has privacy rights to the data, US employees and individuals have far more limited rights. Businesses that are considered the owners of data within their possession will be required to produce this information to opposing parties and the courts.

Various federal and state privacy laws and rules create a patchwork of regulations that govern the management of certain consumer and employee information. This legal patchwork may limit or prevent a company from disclosing protected personal information to third parties, including in discovery. However, the definition of what must be protected and when it must be protected is still far narrower than in other jurisdictions.

One of the more common examples of information that must be protected is personally identifiable health information that the healthcare industry must protect under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Yet, such information may still be required to be produced in certain circumstances. HIPAA includes a provision for the entry of a qualified protective order that allows a party to produce records that contain protected personal health information as long as the records are produced in accordance with the entered qualified protective order.

Another example of information that must be protected is personally identifiable financial information that financial institutions must protect under the Gramm-Leach-Bliley Act of 1999. However, this Act contains a carve-out provision for a financial institution to comply with subpoenas or 'respond to judicial process'.[16] Still, many parties will agree that this information may be redacted from produced documents when the information is irrelevant to the claims or defences in the matter.

16 15 U.S.C. Section 6802(e)(8).

A best practice when producing HIPAA or Gramm-Leach-Bliley protected information is to produce the data in encrypted form to protect against any potential unauthorised disclosure of information. The same can be said for other information that may be protected under various state laws, such as social security numbers, driver's licence numbers and financial account information.

While the United States has not enacted sweeping privacy laws like the European Union's General Data Protection Regulation (GDPR), more jurisdictions within the United States are beginning to assess the need for further data privacy protections. California enacted sweeping consumer data protections under the California Consumer Privacy Act of 2018. This Act provides for a right to know what data is being collected and shared, the right to request deletion of information, and the right to opt out of the sale of personal information to third parties. The city of Chicago is also considering the enactment of a Personal Data Collection and Protection Ordinance.

Moreover, data breaches have been the subject of much scrutiny in Congress, the courts and elsewhere. Numerous class actions have been filed in recent years owing to consumer data breaches. Parties should have plans in place for responding to data breaches implicating personal information.

Even when US privacy laws are not implicated in a matter, owing to increases in data globalisation, companies operating in the global economy are routinely finding that data stored outside the United States is relevant in US legal proceedings. However, obtaining data located outside the United States for US discovery purposes can be problematic. Many countries have laws that protect privacy rights – including in corporate data – and that act as a barrier to US discovery. Data protection laws found throughout much of the rest of the world that limit cross-border transfers of ESI, including in the Asia-Pacific region, the Americas, Europe and the Middle East, do not exist in the United States. As such, many US courts have been resistant to claims that data privacy prevents the disclosure of information in litigation or apply their own understanding of data privacy regulations.[17]

VII OUTLOOK AND CONCLUSIONS

Upcoming changes in e-discovery law will be focused on bringing about the just, speedy and inexpensive determination of matters in accordance with Rule 1. Courts and litigants will continue to look for ways to speed up the e-discovery process while reducing costs. Future e-discovery technologies and AI tools will be aimed at achieving this goal.

Data privacy will continue to be a focus. The intersection between broad-based US discovery and foreign data privacy regulations, such as the GDPR, will continue to play out in courts. Data breaches and privacy concerns could also result in the passage of more stringent regulations governing privacy in various jurisdictions. Even Congressmen from both parties have expressed interest in passing data privacy legislation in 2019.

17 See *Finjan, Inc. v. Zscaler, Inc.*, 2019 WL 618554 (Feb. 14, 2019) (concluding that the GDPR did not preclude discovery).

Appendix 1

ABOUT THE AUTHORS

VICTORIA ARCOS

KLA – Koury Lopes Advogados

Victoria Arcos is an associate at KLA – Koury Lopes Advogados based in São Paulo, Brazil. She is part of the firm's compliance, investigations and white-collar practice group, where her practice focuses on internal investigations in Brazil. She has previous experience working for the Federal Public Prosecutor's Office (MPF). She also has experience assisting Brazilian and multinational clients in significant Brazilian investigations and leniency agreement negotiations.

Victoria participates in issues related to anti-corruption legislation, internal anti-corruption and anti-fraud investigations, multi-jurisdictional investigations, integrity programme reviews, due diligence and background checks. In addition, she reviews companies' internal controls and policies, adjusting them to best practices. She holds a degree in public policy from the University of São Paulo.

REYES BERMEJO BOSCH

Uría Menéndez Abogados, SLP

Reyes Bermejo Bosch is a lawyer in the Madrid office 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, in the preparation of notices, clauses, contracts, protocols and training programmes, in authorisation proceedings for international transfers and administrative and judicial proceedings, preparing 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.

TESS BLAIR

Morgan, Lewis & Bockius LLP

Tess Blair is a litigator and legal entrepreneur who has practised at the intersection of law, technology and design for more than two decades. Tess is the founder and leader of Morgan Lewis's eData practice, a data-driven practice that combines great lawyering with technology and design to enhance the delivery of legal services.

A practising litigator, Tess serves as national discovery counsel to some of the world's largest organisations alongside her client's trial counsel, and as a core member of the litigation team, she develops and executes all aspects of the client's discovery strategy as well as optimising her client's evidence gathering, analysis and presentation. Tess counsels a host of Fortune 500 companies, conducting risk assessments and guiding her clients as they develop internal information governance policies and controls to address privacy, security, retention and disposition of information and data. As leader of eData, Tess works with her team, her colleagues and clients to design and develop tools and techniques to improve the delivery of legal services. The eData team uses process design, automation, UX, product design, application development, machine learning and augmented intelligence tools to develop technology, process and service solutions built to meet clients' needs.

Tess lectures regularly on civil procedure, e-discovery and data privacy – including cross-border discovery and data minimisation – and writes frequently on e-discovery, information governance and data privacy for a variety of legal publications. She is the lead author of the *eData Deskbook*, currently in its third edition. Tess also serves as special discovery master to the Eastern District of Pennsylvania.

PHOEBE BOYLE

Allens

Phoebe Boyle is a lawyer in the disputes and investigations team at Allens with experience in general commercial litigation, including matters at the Supreme Court of New South Wales and the Federal Court. Most recently, Phoebe has had experience working with clients in the technology, media and telecommunications sector, providing advice in relation to privacy, cybersecurity and data governance.

SAMANTHA NAYLOR BROWN

Allens

Samantha Naylor Brown specialises in financial services-related disputes and investigations, including regulatory investigations and the defence of related proceedings. Most recently, Samantha acted for a major financial institution in its response to the Financial Services Royal Commission, managing a team of lawyers and legal technology staff to engage with the Commission. Samantha also works closely with clients on a range of governance- and compliance-related matters, including the implementation of legislative changes, such as the recent introduction of whistle-blower reforms and the banking executive accountability regime in Australia.

OLIVIER DE COURCEL

Feral-Schuhl / Sainte-Marie

Olivier de Courcel works alongside IT clients and suppliers on protecting their copyrights, patents, databases and other intellectual property assets or trade secrets, including in the context of mergers, acquisitions, divestitures and other corporate transactions.

He has extensive experience in drafting and negotiating commercial and intellectual property contracts related to, among other things, software development; licensing; support; integration; outsourcing contracts; reseller, referral and distribution arrangements; cloud computing; and software-as-a-service and other internet services agreements. He also regularly advises businesses on questions relating to website content, advertising, archiving, e-commerce and, more generally, digital services.

In the area of data protection, data privacy and cybersecurity, Olivier provides practical advice on the collection, use, sharing and protection of data, drafts privacy policies and data processing agreements, conducts privacy audits and risk assessments, advises on foreign data protection legislation, and assists companies in responding to data breaches.

Olivier's expertise also includes telecoms regulatory questions, such as licensing issues, access to terrestrial and satellite capacity and frequencies, as well as transactional aspects, such as the sourcing of electronic communications services.

Olivier worked a few years overseas, in Guangdong and in New York, and was previously in-house counsel for major industry actors. He is a member of the Paris and New York Bars.

ROSS DRINNAN

Allens

Ross Drinnan has more than 25 years of experience providing strategic advice to boards and executive teams on a range of commercial disputes. His major work has included class actions, complex commercial disputes, professional negligence and product liability matters. He has also been involved in many regulatory investigations and successfully managed dealings with a broad range of Australian and international regulators.

Ross led a team of lawyers defending the shareholder class action brought against Aristocrat. This was the first matter of its type to proceed to trial in Australia. He has led the defence teams in many other class actions across a diverse range of scenarios.

Ross has also worked with clients on major investigations in Australia – both those that are responsive to regulators and those initiated internally. Ross regularly acts for Westpac, KPMG, Vodafone, Du Pont, Citi, ALE and Aristocrat, among others.

Ross is a director of the Law Council of Australia and a member of the International Association of Defence Counsel, the Defence Research Institute, the International Bar Association and the National Product Liability Association.

ADRIÁN FURMAN

Bomchil

Adrián Furman is a partner in the mergers and acquisitions and entertainment law departments at Bomchil and is in charge of the firm's intellectual property area. He joined the firm in 2000.

He graduated as a lawyer from the University of Buenos Aires in 1998, where he also obtained a postgraduate degree in corporate business law. He is a professor of civil and commercial contracts at the same institution.

He has worked on numerous cross-border transactions and regularly advises corporate clients on various issues of a contractual nature. He also has wide experience on issues of commercial fair trade and consumer protection. During 2005 he was international associate at the New York offices of Simpson Thacher & Bartlett.

He is a frequent speaker at chambers of commerce on his areas of expertise and at the Section of International Law of the American Bar Association seasonal meetings. He has been and is director and auditor of companies such as PepsiCo, AMC Networks, Telefe and Mindray. He is also co-chair of the International Commercial Transactions, Franchising and Distribution Committee of the Section of International Law of the American Bar Association.

His professional performance has been recognised by various specialist publications, including *Chambers Latin America* and *Best Lawyers*, and by the Latin American Corporate Counsel Association and Client Choice Awards.

ANNE GLOVER

Blake, Cassels & Graydon LLP

Anne Glover is a partner at Blake, Cassels & Graydon LLP in Toronto, Canada. Anne is a member of the firm's litigation and dispute resolution group, and the head and founder of Blakes inSource. Anne has extensive expertise in all aspects of electronic discovery and information governance.

ALEXANDER HEIRWEGH

Petillion

Alexander Heirwegh is an associate specialising in intellectual property, information technology, data protection, internet, e-commerce and telecommunications.

Alexander obtained a master's degree in law at Ghent University, *magna cum laude*. He also obtained an LLM in intellectual property and IT law at Leuven University, *magna cum laude*. During his studies, Alexander focused on European and IT law at Charles University in Prague, Czech Republic, while taking part in the Erasmus exchange programme.

Alexander has a particular expertise in online brand and copyright protection, and domain names. He has participated in various online trademark and copyright infringement cases, and domain name disputes.

He has written a master's thesis on privacy and trademark enforcement issues in cybersquatting cases.

JAN JANSSEN

Petillion

Jan Janssen is a senior dispute resolution lawyer and arbitrator with a keen interest in complex regulatory matters and technology. He specialises in commercial and international arbitration with a focus on intellectual property, information technology and the liberalisation of sectors.

Jan's practice primarily involves complex civil litigation and commercial arbitration in a variety of industries, including fashion, media, postal services, technology and telecommunications.

Jan also provides contractual advice and assists clients in protecting, managing and enforcing their intellectual property rights in both an online and offline environment. He assists and represents clients in transactional matters, such as distribution, agency, licensing, technology transfer, software development, outsourcing and service level agreements.

MAJA KARCZEWSKA

Kobylańska & Lewoszewski Kancelaria Prawna Sp. j.

Maja Karczewska is an advocate trainee at the District Bar Council in Warsaw. Her main areas of interest include media and advertising law and intellectual property law, with particular emphasis on copyright. She also provides legal services in the field of personal data protection.

She studied at the faculty of law and administration at the University of Warsaw and graduated with honours (thesis topic: 'Limits of the freedom of artistic expression'). She was also a student at the Centre for American Law, a joint initiative of the faculty of law and administration at the University of Warsaw and Levin College of Law, as well as an intellectual property school organised by the faculty of law and administration at the Jagiellonian University (Krakow Intellectual Property Law Summer School 2017).

ANNA KOBYLAŃSKA

Kobylańska & Lewoszewski Kancelaria Prawna Sp. j.

Anna Kobylańska is an advocate and member of the District Bar Chamber in Warsaw. Prior to establishing her own law firm, for more than 10 years she practised intellectual property, new technologies and personal data protection law in international law firms.

Anna specialises in legal counselling in the field of personal data protection, copyright, industrial property rights, media and advertising law, and the law of new technologies. She has many years of experience in leading projects relating to internet domain protection, use of new technologies to collect and process personal data (internet of things, big data, behavioural targeting) and IT systems implementation. She also participated in projects concerning the assessment of the potential of technology start-ups in the context of the intellectual property generated by them. As regards the implementation of the EU GDPR requirements, she has worked for clients in the financial, media, automotive, retail and business consulting sectors.

She is the author of *Protection of Trademarks on the Internet* and co-author of *Data Protection in Business Practices* and *Protection of Trademarks: Online Use and Anticybersquatting – A European Perspective*, which are the first books of their kind in Poland. She lectures at the Grotius Centre for Intellectual Property. For a number of years, she has been involved in the works of the International Trademark Association (INTA) committees, including, in 2016–2017, in the Personal Data Protection Committee. She is a member of the International Association of Privacy Professionals.

In 2017, Anna's data protection law practice was distinguished in the regulatory law firms ranking published by *Polityka Insight*. Since 2012, Anna has also been ranked each year in *Chambers Europe* in the 'TMT: Data Protection' area.

MARCIN LEWOSZEWSKI

Kobylańska & Lewoszewski Kancelaria Prawna Sp. j.

Marcin Lewoszewski is a legal counsel, member of the Warsaw Bar Association. Before establishing his own law firm, he worked for more than seven years in the TMT team with one of the leading international law firms based in Warsaw. For two years before that, he worked at the Inspector General for Personal Data Protection (GIODO).

Marcin specialises in legal advice on personal data protection and the law of new technologies, including the provision of electronic services, database protection, gambling, IT systems implementation and telecommunications law. He has advised clients in locating data processing centres in Poland and participated in creating one of the largest online business-to-business trading platforms in Poland. He has many years of experience in leading projects aimed at adapting business practices to the requirements of data protection law. On numerous occasions, he represented clients in proceedings conducted by GIODO, including for the acceptance of binding corporate rules by the supervisory authority, and in connection with GIODO inspections. His experience includes negotiating database licence agreements and advising clients on the legal aspects of obtaining data from publicly available records. His professional interests focus on selected sectors of the economy, primarily pharmaceuticals, e-commerce, new technologies and media.

Author of dozens of articles on personal data protection, Marcin has been published in the Polish edition of the *Harvard Business Review*, *Rzeczpospolita* and *Dziennik Gazeta Prawna*, and abroad in Bloomberg BNA, IAPP Privacy Tracker and DataGuidance. Together with Anna Kobylańska and Maja Karczewska, he co-authored a chapter on Polish data protection law in *The Privacy, Data Protection and Cybersecurity Law Review*. He has often been quoted by the press in Poland and abroad, including by Politico.

In 2016, he was appointed co-chair of IAPP Knowledge NET Poland by the International Association of Privacy Professionals, a global organisation gathering personal data protection professionals. *Dziennik Gazeta Prawna* nominated him as one of the 30 most promising lawyers before 35 in Poland.

CATALINA MALARA

Bomchil

Catalina Malara is a member of the mergers and acquisitions and entertainment law departments at Bomchil. She graduated with honours from the University of Buenos Aires in 2016.

MICHAEL MORRIS

Allens

Michael Morris specialises in all corporate, commercial and regulatory aspects of technology, telecommunications, intellectual property and the data life cycle. He has 20 years' experience across a range of ICT-sector, IP and data issues in Australia, Europe, Singapore and Papua New Guinea.

He is particularly experienced in large projects that involve the procurement or outsourcing of ICT, business process outsourcing, ICT system separations, business transformation, and corporate transactions and projects in the ICT sector and data market.

He also regularly advises clients across all industry sectors and government on cybersecurity issues, data protection, data commercialisation, data governance, dealing with data breaches, IP protection and IP commercialisation.

KRZYSZTOF MUCIAK

Kobylańska & Lewoszewski Kancelaria Prawna Sp. j.

Krzysztof Muciak is an advocate and member of the Warsaw Bar Association. Before joining Kobylańska & Lewoszewski, he worked at several Polish and international law firms. He graduated from the faculty of law and administration at the University of Warsaw, and the British Law Centre (part of the same faculty). He completed postgraduate studies in cybersecurity management at the Warsaw School of Economics.

Krzysztof specialises in advising clients in matters regarding personal data protection and cybersecurity. He also has experience in providing day-to-day advice to commercial entities, including in the scope of rendering services via the internet and consumer rights regulations.

Krzysztof has several years of experience in conducting audits of businesses and non-governmental organisations regarding compliance of their operations with personal data protection regulations, as well as in implementing requirements of the EU General Data Protection Regulation. He conducted comprehensive implementation projects where he drafted required internal and external documents, negotiated contracts regarding personal data entrustment and transfer to states outside the European Union, and carried out training courses for the staff and managers of his clients. He advised business clients from various market sectors, including transport, IT, schooling, consulting, retail sales and production. He is the author of several articles on data protection issues, including publications on the GDPR, e-privacy and processing data, including in cookie files.

DIÉGO NOESEN

Petillion

Diégo Noesen is a member of the intellectual property, information technology and media team. He is a senior dispute resolution lawyer focusing on European and domestic litigation with an emphasis on intellectual property. Diégo's practice involves complex civil litigation in a variety of industries and sectors, including media and entertainment, fashion, automotive, technology and telecommunications.

Diégo also provides transactional advice and assists clients in protecting, managing and enforcing their intellectual property rights. He has a particular expertise in brand and copyright protection, and domain names.

DANILO ORENGA

KLA – Koury Lopes Advogados

Danilo Orenga is an associate at KLA – Koury Lopes Advogados based in São Paulo, Brazil. He has experience in conducting complex litigation cases in various types of claims, such as contracts matters, franchising disputes, competition, consumer, insurance, advertising and publicity claims. He started his career in 2008 at KLA. Danilo Orenga has a postgraduate degree in contractual law from the renowend Getúlio Vargas Foundation and is currently pursuing his master's degree in civil law at the Pontifical Catholic University of São Paulo.

FLIP PETILLION

Petillion

Flip Petillion is a leading domestic and international litigator and arbitrator.

Flip has been handling court litigations and arbitrations for 30 years. Matters were related to different industries. He has built an outstanding reputation through his special focus on intellectual property rights, information, communication, technology and media.

He represents multinationals and first-class individual portfolio holders.

Flip is the founder of Petillion. It is a boutique firm focusing on dispute resolution. The firm acts in Belgian courts and before the European Court of Justice and the European General Court.

ELOY RIZZO

KLA – Koury Lopes Advogados

Eloy Rizzo is a partner at KLA – Koury Lopes Advogados based in São Paulo, Brazil. He is the vice chair of the firm's compliance, investigations and white-collar practice group, where his practice focuses on internal investigations related primarily to the Brazilian anti-corruption legislation and associated litigation matters. He has assisted companies from around the world with multi-jurisdictional investigations and has special expertise with US–Brazil cross-border investigations (ranked in *Chambers Global* and *Chambers Latin America* as Band 4 in Compliance). In 2015, Rizzo spent 10 months as a visiting associate in the FCPA and international anti-corruption practice group at Miller & Chevalier in Washington, DC.

He has extensive experience in conducting complex investigations focused on potential violation of anti-corruption laws, including the FCPA and UKBA in multi-jurisdictional cases. In addition, Eloy is a leader in training management and employees, conducting compliance risk assessments, and dealing with administrative and judicial proceedings arising out of violations of anti-corruption legislation. He holds an LLB from the Faculty of Law of the Pontifical Catholic University of São Paulo and an LLM from the University of London, King's College.

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 others. 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 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, in 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 others). She has also experience in advising companies on the development and implementation of compliance programmes, as well as on conducting internal investigations.

AFZALAH SARWAR

Morgan, Lewis & Bockius UK LLP

Afzalah Sarwar focuses on complex commercial matters involving both litigation and arbitration, and counsels and advises companies in electronic disclosure and information governance processes. Afzalah represents both public and private companies, multinational corporations, banks, private equity firms and others in matters including multi-jurisdictional contractual and banking disputes, and government investigations. Afzalah has represented clients in both English High Court and Court of Appeal proceedings, and before various arbitral bodies.

KENTARO TODA

TMI Associates

Kentaro Toda is a partner at TMI Associates. He provides legal services in international disputes (including supporting discovery in foreign litigation); competition laws; foreign bribery regulations; and international trade issues (anti-dumping, economic sanctions, CFIUS, etc.). In addition to supporting clients in multi-jurisdiction complex civil litigation, he has counselled various companies, officers and employees in the area of competition, and is familiar with the practice of handling investigations conducted by competition authorities in various jurisdictions, including Japan, the United States and Europe, and with civil actions in foreign countries including class actions. Additionally, he has worked on many cases requiring merger filings in multi-jurisdictional matters, and is experienced in the merger filing practices of global M&A cases. He has in-depth knowledge of anti-dumping taxation investigations, and has counselled producers, importers and users with regard to investigations conducted by the Japanese government; producers with regard to investigations conducted by foreign authorities; and other relevant authorities. In addition, he vigorously engages in providing advice concerning the establishment of global compliance systems and serves as a lecturer at in-house training sessions on compliance.

MARTÍN TORRES GIROTTI

Bomchil

Martín Torres Girotti joined Bomchil in 2004 and has developed a strong practice in litigation. His practice focuses on complex civil and commercial disputes, both litigation and arbitration, in connection with contractual, financial, corporate and insurance matters, class

actions and end-product liability, among other issues. He also advises and represents national and foreign clients in reorganisations and insolvency, and in out-of-court debt restructuring proceedings.

He is a professor of reorganisations and insolvency at the School of Law of the University of Buenos Aires and a professor of the postgraduate programme at the Catholic University of Argentina.

Martín Torres Girotti holds a law degree from the Catholic University of La Plata (1998 and 1999) and qualified as a notary at the same institution. He holds a master's degree in finance from the University of CEMA (2003).

As a specialist in his practice area, he has been acknowledged numerous times by *Chambers Latin America*.

JENNIFER MOTT WILLIAMS

Morgan, Lewis & Bockius LLP

Jennifer Mott Williams helps clients develop and implement efficient ways to manage increasingly challenging electronic discovery processes. She advises clients on end-to-end discovery processes, including litigation holds and preservation, ESI protocols, collection strategies, data culling and iterative search term processes, and the overall document review and production process. Jennifer works closely with clients to implement best practices for information governance, including data retention and disposition, remote worksite policies, and strategies to protect key information assets.

Appendix 2

CONTRIBUTORS' CONTACT DETAILS

ALLENS

Level 28, Deutsche Bank Place
126 Phillip Street
(Corner Hunter & Phillip Streets)
Sydney NSW 2000
Australia
Tel: +61 2 9230 4000
Fax: +61 2 9230 5333
ross.drinnan@allens.com.au
michael.morris@allens.com.au
samantha.naylorbrown@allens.com.au
phoebe.boyle@allens.com.au
www.allens.com.au

BLAKE, CASSELS & GRAYDON LLP

199 Bay Street
Suite 4000, Commerce Court West
Toronto ON M5L 1A9
Canada
Tel: +1 416 863 2400
Fax: +1 416 863 2653
anne.glover@blakes.com
www.blakes.com

BOMCHIL

Corrientes Avenue 420, 3rd Floor
C1043 AAR Buenos Aires
Argentina
Tel: +54 11 4321 7500
Fax: +54 11 4321 7555
adrian.furman@bomchil.com
martin.torres@bomchil.com
catalina.malara@bomchil.com
www.bomchil.com.ar

FÉRAL-SCHUHL / SAINTE-MARIE

24, rue Erlanger
75016 Paris
France
Tel: +33 1 70 71 22 00
Fax: +33 1 70 71 22 22
odecourcel@feral-avocats.com
www.feral-avocats.com

KLA – KOURY LOPES ADVOGADOS

Av. Brigadeiro Faria Lima, 1355, 18°
São Paulo, SP
01452–919
Brazil
Tel: +55 11 3799 8158 / 8271 / 8188
erizzo@klalaw.com.br
dorenga@klalaw.com.br
varcos@klalaw.com.br
www.klalaw.com.br

KOBYLAŃSKA & LEWOSZEWSKI KANCELARIA PRAWNA SP. J.

ul. Śniadeckich 10
00–656 Warsaw
Poland
Tel: +48 604 817 352
anna.kobylanska@klattorneys.pl
marcin.lewoszewski@klattorneys.pl
krzysztof.muciak@klattorneys.pl
maja.karczewska@klattorneys.pl
www.klattorneys.pl

MORGAN, LEWIS & BOCKIUS LLP

1701 Market Street
Philadelphia, PA
19103–2921
United States
Tel: +1 215 963 5161 (direct)
+1 215 260 2660 (mobile)
+1 215 963 5000 (main)
tess.blair@morganlewis.com

1000 Louisiana Street, Suite 4000
Houston, TX
77002–5005
United States
Tel: +1 713 890 5788 / 5000
Fax: +1 713 890 5001
jennifer.williams@morganlewis.com

Morgan, Lewis & Bockius UK LLP
Condor House
5-10 St Paul's Churchyard
London EC4M 8AL
United Kingdom
Tel: +44 20 3201 5659 / 5000
Fax: +44 20 3201 5001
afzalah.sarwar@morganlewis.com

www.morganlewis.com

PETILLION

Guido Gezellestraat 126
1654 Huizingen
Belgium
Tel: +32 2 306 18 60
Fax: +32 2 306 18 69
fpetillion@petillion.law
jjanssen@petillion.law
dnoesen@petillion.law
aheirwegh@petillion.law
www.petillion.law

TMI ASSOCIATES

23rd Floor, Roppongi Hills Mori Tower
6-10-1 Roppongi
Minato-ku
Tokyo 106-6123
Japan
Tel: +81 3 6438 5511 / 5692
Fax: +81 3 6438 5522
ktoda@tmi.gr.jp
www.tmi.gr.jp

URÍA MENÉNDEZ ABOGADOS, SLP

c/Príncipe de Vergara, 187
Plaza de Rodrigo Uria
28002 Madrid
Spain
Tel: +34 915 860 579
enrique.rodriguez@uria.com
sara.sanz@uria.com
reyes.bermejo@uria.com
www.uria.com

THE LAW REVIEWS

For more information, please contact info@thelawreviews.co.uk

THE ACQUISITION AND LEVERAGED FINANCE REVIEW
Marc Hanrahan
Milbank Tweed Hadley & McCloy LLP

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW
Mark F Mendelsohn
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE ASSET MANAGEMENT REVIEW
Paul Dickson
Slaughter and May

THE ASSET TRACING AND RECOVERY REVIEW
Robert Hunter
Edmonds Marshall McMahon Ltd

THE AVIATION LAW REVIEW
Sean Gates
Gates Aviation LLP

THE BANKING LITIGATION LAW REVIEW
Christa Band
Linklaters LLP

THE BANKING REGULATION REVIEW
Jan Putnis
Slaughter and May

THE CARTELS AND LENIENCY REVIEW
John Buretta and John Terzaken
Cravath Swaine & Moore LLP and Simpson Thacher & Bartlett LLP

THE CLASS ACTIONS LAW REVIEW
Camilla Sanger
Slaughter and May

THE COMPLEX COMMERCIAL LITIGATION LAW REVIEW
Steven M Bierman
Sidley Austin LLP

THE CONSUMER FINANCE LAW REVIEW
Rick Fischer, Obrea Poindexter and Jeremy Mandell
Morrison & Foerster

THE CORPORATE GOVERNANCE REVIEW
Willem J L Calkoen
NautaDutilh

THE CORPORATE IMMIGRATION REVIEW
Chris Magrath
Magrath LLP

THE CORPORATE TAX PLANNING LAW REVIEW
Jodi J Schwartz and Swift S O Edgar
Wachtell, Lipton, Rosen & Katz

THE DISPUTE RESOLUTION REVIEW
Damian Taylor
Slaughter and May

THE DOMINANCE AND MONOPOLIES REVIEW
Maurits J F M Dolmans and Henry Mostyn
Cleary Gottlieb Steen & Hamilton LLP

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW
Tess Blair
Morgan, Lewis & Bockius LLP

THE EMPLOYMENT LAW REVIEW
Erika C Collins
Proskauer Rose LLP

THE ENERGY REGULATION AND MARKETS REVIEW
David L Schwartz
Latham & Watkins

THE ENVIRONMENT AND CLIMATE CHANGE LAW REVIEW
Theodore L Garrett
Covington & Burling LLP

THE EXECUTIVE REMUNERATION REVIEW
Arthur Kohn and Janet Cooper
Cleary Gottlieb Steen & Hamilton LLP and Tapestry Compliance

THE FINANCIAL TECHNOLOGY LAW REVIEW
Thomas A Frick
Niederer Kraft Frey

THE FOREIGN INVESTMENT REGULATION REVIEW
Calvin S Goldman QC
Goodmans LLP

THE FRANCHISE LAW REVIEW
Mark Abell
Bird & Bird LLP

THE GAMBLING LAW REVIEW
Carl Rohsler
Memery Crystal

THE GLOBAL DAMAGES REVIEW
Errol Soriano
Duff & Phelps

THE GOVERNMENT PROCUREMENT REVIEW
Jonathan Davey and Amy Gatenby
Addleshaw Goddard LLP

THE HEALTHCARE LAW REVIEW
Sarah Ellson
Fieldfisher LLP

THE INITIAL PUBLIC OFFERINGS LAW REVIEW
David J Goldschmidt
Skadden, Arps, Slate, Meagher & Flom LLP

THE INSOLVENCY REVIEW
Donald S Bernstein
Davis Polk & Wardwell LLP

THE INSURANCE AND REINSURANCE LAW REVIEW
Peter Rogan
Ince & Co

THE INSURANCE DISPUTES LAW REVIEW
Joanna Page
Allen & Overy LLP

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW
Thomas Vinje
Clifford Chance LLP

THE INTELLECTUAL PROPERTY REVIEW
Dominick A Conde
Fitzpatrick, Cella, Harper & Scinto

THE INTERNATIONAL ARBITRATION REVIEW
James H Carter
Wilmer Cutler Pickering Hale and Dorr

THE INTERNATIONAL CAPITAL MARKETS REVIEW
Jeffrey Golden
P.R.I.M.E. Finance Foundation

THE INTERNATIONAL INVESTIGATIONS REVIEW
Nicolas Bourtin
Sullivan & Cromwell LLP

THE INTERNATIONAL TRADE LAW REVIEW
Folkert Graafsma and Joris Cornelis
Vermulst Verhaeghe Graafsma & Bronckers (VVGB)

THE INVESTMENT TREATY ARBITRATION REVIEW
Barton Legum
Dentons

THE INWARD INVESTMENT AND INTERNATIONAL TAXATION REVIEW
Tim Sanders
Skadden, Arps, Slate, Meagher & Flom LLP

THE ISLAMIC FINANCE AND MARKETS LAW REVIEW
John Dewar and Munib Hussain
Milbank Tweed Hadley & McCloy LLP

THE LABOUR AND EMPLOYMENT DISPUTES REVIEW
Nicholas Robertson
Mayer Brown

THE LENDING AND SECURED FINANCE REVIEW
Azadeh Nassiri
Slaughter and May

THE LIFE SCIENCES LAW REVIEW
Richard Kingham
Covington & Burling LLP

THE MERGER CONTROL REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE MERGERS AND ACQUISITIONS REVIEW
Mark Zerdin
Slaughter and May

THE MINING LAW REVIEW
Erik Richer La Flèche
Stikeman Elliott LLP

THE OIL AND GAS LAW REVIEW
Christopher B Strong
Vinson & Elkins LLP

THE PATENT LITIGATION LAW REVIEW
Trevor Cook
WilmerHale

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW
Alan Charles Raul
Sidley Austin LLP

THE PRIVATE COMPETITION ENFORCEMENT REVIEW
Ilene Knable Gotts
Wachtell, Lipton, Rosen & Katz

THE PRIVATE EQUITY REVIEW
Stephen L Ritchie
Kirkland & Ellis LLP

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW
John Riches
RMW Law LLP

THE PRODUCT REGULATION AND LIABILITY REVIEW
Chilton Davis Varner and Madison Kitchens
King & Spalding LLP

THE PROFESSIONAL NEGLIGENCE LAW REVIEW
Nick Bird
Reynolds Porter Chamberlain LLP

THE PROJECT FINANCE LAW REVIEW
David F Asmus
Sidley Austin LLP

THE PROJECTS AND CONSTRUCTION REVIEW
Júlio César Bueno
Pinheiro Neto Advogados

THE PUBLIC COMPETITION ENFORCEMENT REVIEW
Aidan Synnott
Paul, Weiss, Rifkind, Wharton & Garrison LLP

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW
Bruno Werneck and Mário Saadi
Mattos Filho, Veiga Filho, Marrey Jr e Quiroga Advogados

THE REAL ESTATE LAW REVIEW
John Nevin
Slaughter and May

THE REAL ESTATE M&A AND PRIVATE EQUITY REVIEW
Adam Emmerich and Robin Panovka
Wachtell, Lipton, Rosen & Katz

THE RENEWABLE ENERGY LAW REVIEW
Karen B Wong
Milbank

THE RESTRUCTURING REVIEW
Christopher Mallon
Skadden, Arps, Slate, Meagher & Flom LLP

THE SECURITIES LITIGATION REVIEW
William Savitt
Wachtell, Lipton, Rosen & Katz

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW
Francis J Aquila
Sullivan & Cromwell LLP

THE SHIPPING LAW REVIEW
George Eddings, Andrew Chamberlain and Rebecca Warder
HFW

THE SPORTS LAW REVIEW
András Gurovits
Niederer Kraft Frey

THE TAX DISPUTES AND LITIGATION REVIEW
Simon Whitehead
Joseph Hage Aaronson LLP

THE TECHNOLOGY, MEDIA AND TELECOMMUNICATIONS REVIEW
John P Janka
Latham & Watkins

THE THIRD PARTY LITIGATION FUNDING LAW REVIEW
Leslie Perrin
Calunius Capital LLP

THE TRADEMARKS LAW REVIEW
Jonathan Clegg
Cleveland Scott York

THE TRANSFER PRICING LAW REVIEW
Steve Edge and Dominic Robertson
Slaughter and May

THE TRANSPORT FINANCE LAW REVIEW
Harry Theochari
Norton Rose Fulbright

THE VIRTUAL CURRENCY REGULATION REVIEW
Michael S Sackheim and Nathan A Howell
Sidley Austin LLP

www.TheLawReviews.co.uk

ISBN 978-1-912228-76-8