THE e-Discovery and Information Governance Law Review

Second Edition

Editor
Jennifer Mott Williams

THE LawReviews

THE E-DISCOVERY AND INFORMATION GOVERNANCE LAW REVIEW

SECOND EDITION

Reproduced with permission from Law Business Research Ltd
This article was first published in June 2020
For further information please contact Nick.Barette@thelawreviews.co.uk

Editor
Jennifer Mott Williams

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

PRODUCTION AND OPERATIONS DIRECTOR
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Gillian Fraser

CHIEF EXECUTIVE OFFICER
Nick Brailey

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

www.TheLawReviews.co.uk

ISBN 978-1-83862-447-7

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

ACKNOWLEDGEMENTS

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

ALLENS

BOMCHIL

DEMAREST ADVOGADOS

FÉRAL-SCHUHL / SAINTE-MARIE

KOBYLAŃSKA LEWOSZEWSKI MEDNIS SP J

MORGAN, LEWIS & BOCKIUS LLP

PETILLION

TMI ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

CONTENTS

PREFACE

Virtually unheard of 20 years ago, increasing data volumes and ever-changing technologies have resulted in e-discovery and information governance exploding onto the legal scene. Corporations face a wide array of overlapping and competing e-discovery and information governance laws and regulations impacting the use, retention and disposition of electronically stored information (ESI). This second 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.

Recent global events have further complicated data privacy. The covid-19 pandemic is causing many jurisdictions to amend their data privacy laws in pursuit of the common good. However, whether jurisdictions will extend such laws following the pandemic's end and what will happen to data collected during the pandemic has yet to be determined.

Information governance is likewise an intricate issue, involving the organisation, maintenance, use and disposition of information in light of business goals, as well as complex legal and regulatory obligations. Effective information governance provides an organisation with an opportunity to control ever-expanding data volumes as well as newer technologies and forms of ESI. It also provides corporations with knowledge and insight into their own data assets so that they know what information they have, where it is kept and how it is being used. Information governance further includes having processes in place for handling sensitive information that may be governed by various data protection laws or other regulations. With more employees working remotely throughout the world, the recent covid-19 pandemic has caused many businesses to reassess their information governance policies.

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

Jennifer Mott Williams
Morgan, Lewis & Bockius LLP
Houston
April 2020

Chapter 6

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 discovery phase is launched pretrial, that is, before the contradictory examination of the parties' legal claims, with a variety of means of proof, such as interrogations, depositions, applications for admission and requests for the production of documents.

Further, 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 then 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. Finally, 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. 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 (see Section IV). The disclosure and examination of evidence usually goes along with the examination of the legal claims of the parties. Therefore, a discovery phase will take place separately, before trial, only if a party specifically applies for it and the judge agrees to it.

Since there is no general obligation to disclose documents requested by the opposing party (see Section IV), under civil procedural rules there is also no general obligation to preserve evidence (including electronically stored data) in anticipation of a trial. Conversely, in areas of the law that are subject to administrative or criminal sanctions (e.g., taxes, antitrust, financial markets, telecommunications, criminal law), special texts impose retention periods for certain types of documents, which means that companies must preserve predefined evidence in order to be able to produce it when so requested by investigators. In this area, recent developments in digitisation and archiving, investigation techniques and digital surveillance raise issues similar to those met with e-discovery, such as the breadth of electronic data that may be legally accessible and the use of forensic software.

These developments can be explained by the fact that, in relationships between merchants, commercial law leaves the parties freedom of proof, whether on paper or in

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). See chapter 11, page 94.

digital form, while in legal areas subject to administrative or judicial control, the possibility of applying administrative or criminal sanctions requires more precise rules to govern the content of investigations as well as the scope of data accessible by electronic means and admissible as evidence.

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) may undergo significant development when the draft EU e-Evidence Regulation, dated 17 April 2018, makes its way through the Union legislative process.[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 need 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, 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 would 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.

All injunctions issued under this procedure would 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 could only be issued after an assessment of its proportionality and necessity in the particular case under consideration. One of the questions explaining the (very) slow process of adoption is whether and how far the courts of the Member State in which the provider is established should be able to review the disclosure order issued by the judge in charge of the investigation in the initial Member State.

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.

III CONTROL AND PRESERVATION

i Duties to preserve evidence

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 judges 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.

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 L123-22) 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.[7] In this respect, the Tax Administration specifies that a failure to keep records, whether totally or partially, that is noticed by the Administration's agents may therefore be sanctioned. For example, failure to keep original invoices in electronic form may lead to VAT deductions being repelled.[8]

In other specific areas, special texts provide for similar obligations to keep documents for a fixed period of time, including in electronic form. Thus, under labour law, such an obligation applies, for example, to the single personnel register and to employers' declarations of accidents at work.[9] Similarly, electronic communications operators must keep traffic and other technical data of their users for one year.[10]

In principle, a party to a civil case cannot rely on the special texts to request the evidence they provide for. Exceptions are made, for example, to allow the disclosure of accounting documents in court in cases of succession, community, company sharing, judicial reorganisation or liquidation.[11] A party may also ask a judge to request a telecom operator to disclose technical data necessary to sustain a claim, for instance to disclose the IP address of the author of defamatory comments on a social network.

ii Order to preserve evidence in anticipation of litigation

In this context, a duty to keep documents specifically in anticipation of a trial will only arise by decision of a judge. Before a trial, a plaintiff may indeed apply to the judge for an order for any legally admissible investigation measure, which includes the possibility to require the

7 Article L102 B et seq. of the Tax Procedures Book.

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

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

10 Postal and Electronic Communications Code, Article L34-1

11 Commercial Code, Article L123-23.

opposing party or a third party to retain or disclose evidence in view of a trial. This measure is known as *in futurum*, as it allows the plaintiff to request the preservation of evidence that it may use thereafter at trial before the court (Code of Civil Procedure (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.[12]

Also prior to trial, when a business is subject to control by administrative or regulatory authorities, it must retain all information (in whatever form) that may be requested by the investigators. In this regard, the Paris Court of Appeal refers 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'.[13] This duty to keep records concerns 'not only the accounting documents and supporting documents provided for in Article L123-22 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'.

iii Sanctions for failure to preserve evidence

Under ordinary law, failure to keep documents is not punishable. An exception is made under criminal law: destroying, diverting, concealing or altering a public or private document or an object likely to facilitate the discovery of a crime or misdemeanour, the search for evidence or the conviction of guilty parties in order to obstruct the establishment of the truth may be punished by three years' imprisonment and a fine of €45,000.[14] Regarding administrative or regulatory proceedings, certain special texts (e.g., the General Tax Code) provide for specific sanctions.

IV REQUESTS AND SCOPE

i Request to the judge

According to Article 9 of the 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. Conversely, a party is not required to systematically disclose all the elements that may serve as evidence in the dispute in question.

In this context, if a party wants to obtain materials from its opponent or from a third party, it must request them from the judge, and the communication of such documents must then be decided by a judge order (possibly delivered *ex parte*). As a consequence, absent a procedure equivalent to discovery, the parties to a trial do not have to meet and confer in advance on the evidence they will produce.

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

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

14 Penal Code, Article 434-4.

ii The judge's order

When ruling on a party's request for evidence, a judge may order such communication and make it subject to a daily penalty in an amount that the judge's order will fix. The judge may also order, on his or her own initiative or at the request of a party, 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 words, to establish proof of facts that the applicant is not in a position to establish totally or alone.

The criminal procedure rules take more specific account of electronic evidence than the civil rules. The means of accessing electronic communications and electronically stored evidence have recently been strengthened on the grounds of the fight against terrorism.[15] In general, electronic evidence can be searched for by criminal investigators via warrant procedures (e.g., for technical records, location data and current e-correspondence), including search warrants (to access stored data, including past correspondence).

iii Proportionality and loyalty of evidence

Case law prohibits investigation measures that are general. Such was the case, for example, of a discovery order reversed in 2012 that '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]'. More specifically, judges exclude measures that exceed the needs of the case and whose purpose is not limited in space and time.

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.[16]

In the field of intellectual property, when evidence of counterfeiting is being sought, the right holder may request a court order to authorise a bailiff to describe and take a copy of an allegedly infringing piece of software or database. Making a copy is obviously less burdensome and risky for both parties than seizing the production instance of the program or database.[17]

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 also on evidence that has been illegally obtained, as long as that evidence has been open to debate in a fair trial.[18]

15 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.

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

17 Intellectual Property Code, Article L332-4.

18 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

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,[19] which constitutes an unfair process and is therefore not admissible as evidence (but would be admissible before a criminal court).[20] This only concerns evidence used by civil parties: in criminal cases, investigators must comply with the principle of fair evidence.[21]

When called upon to assess the proportionality and fairness of the disclosure requested, a court will consider not only the interest of the applicant, but also the protection of fundamental freedoms (in particular the right to privacy) and of secrets protected by law (in particular professional and business secrecy) (see Section V).

In the area of criminal discovery, the Criminal Procedure Code allows investigators to access data from a computer system located on the premises where a search takes place. The search warrant may also cover data stored in a remote computer system, 'as long as such data is accessible from the initial system or available to the initial system'. However, the Criminal Procedure Code reserves the duty to comply with international treaties, which govern authorities' access to data collected when a remote computer system is located outside the national territory.[22]

iv Failure to provide evidence

The judge is in charge of controlling the timing of the proceedings. Before concluding the preliminary phase of a trial (exchange of pleadings) and summoning the parties to the hearings, 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. It remains contingent on the judge's decision, on a case-by-case basis, to draw the consequences of a party's possible bad faith in refusing to provide such evidence.

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.

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'.

19 '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).

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

21 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).

22 Code of Criminal Procedure, Article 57-1.

V REVIEW AND PRODUCTION

i Production

As French civil procedure law does not provide for a general obligation to communicate to the opposing party the documents relevant to a 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.[23] 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.'[24]

These provisions do not allow investigators to request, in a general and imprecise manner, all documents located in a 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'.[25] 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, in as far as email files cannot be split.[26]

ii Admissibility

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 this data is 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 France as elsewhere, attorney consultations, attorney–client correspondence and attorney meeting notes are covered by attorney–client privilege. Whether they appear on paper or in electronic format, such documents cannot be requested as evidence; nor would they be admissible if inadvertently communicated. 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.[27]

23 Other specific areas regulated by supervisory authorities have seen similar developments in the right of investigators to communicate: see, for example, in the pharmaceutical sector (Public Health Code, Article L1421-3; in matters of consumer protection (Consumer Code, Article L512-11); and in financial control (Code of Financial Courts, Article R241-1 et seq.).

24 EU Directive 2016/943 of 8 June 2016, transposed into the Commercial Code, Article L450-3 and L 450-4.

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

26 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 email file, unless its content is altered, is unbreakable'.

27 Rules of Professionnal Conduct, Article 2

This protection against discovery may be more effective than in other jurisdictions, though, in as far as an attorney's professional secrecy is protected as a fundamental right under the European Convention for the Protection of Human Rights and Fundamental Freedoms, meaning that disclosure of information may only be required by law under certain conditions. Thus, in matters of corruption and money laundering, for example, information obtained by a French attorney in the course of assessing the legal situation of a client is excluded from the scope of the obligations of information and cooperation in relation to public authorities, save only in cases such as where the lawyer takes part in such activities.[28]

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.*[29]

Similarly, judges may put aside a claim for attorney–client privilege applicable abroad when such protection is not applicable under French law.[30]

The principles of secrecy of correspondence and fair evidence offer other legal grounds to challenge a too-large request or use of evidence by the other party in civil matters. Thus, an appeal decision overturned 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.[31] 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.[32] Before this text, a party could ask a civil judge to order an investigation measure, if necessary in a non-adversarial manner (CPC, Article 145), in order 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.

28 ECJ, 26 June 2007, No. C-305-05, Ordre des barreaux francophones et germanophones et autres

29 ibid.

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

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

32 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.

In the European Union, personal data is indeed considered as a personal right belonging to the person identifiable by such data (right *in personam*) more than as a proprietary right belonging to the person holding such data. Therefore, third parties holding personal data cannot freely disclose it.

In this respect, both the EU General Data Protection Regulation (GDPR) and the French Computer and Freedoms Act[33] prohibit, in principle, the transfer of personal data to countries whose legislation does not offer an equivalent level of protection as that provided by the laws of the Union. 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.[34]

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 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 legal assistance treaty.

In France, as in the United States and elsewhere, the procedure applicable to civil and business relationships consists of international letters rogatory as provided for by the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil and Commercial Matters (Hague 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 Hague Convention, France has declared that it will not will not comply with international letters rogatory 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.

33 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 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.

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

Since the 1987 Supreme Court *Aérospatiale* judgment,[35] US courts have considered civil judicial cooperation proceedings under the Convention to be optional – that is, not superseding the extraterritorial application of the US pretrial discovery rules.

France and the United States are also bound by a mutual legal assistance treaty in criminal matters, signed on 10 December 1998 and ratified in 2000. The European Union and the United States also signed an agreement, in June 2003, providing for mutual legal assistance to search and communicate banking information and to create joint investigative teams.[36]

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 proportionality (i.e., they will require that only personal data necessary for a procedure be disclosed).

The French Data Protection Authority and the European Coordination Committee recommend in this respect to:

a provide anonymised or pseudonymised data, where possible; and

b request (via stipulative court orders) to limit the scope of the documents 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.[37]

The same authorities recommend, for companies that may be subject to an international 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) about 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 that 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.[38]

35 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).

36 Agreement on mutual legal assistance between the European Union and the United States of America, 25 June 2003, No 22003A0719(02).

37 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.

38 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).

In all cases, the persons whose data is 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.[39]

In view of the extraterritorial and intrusive nature of cross-border discovery procedures, the French authorities have adopted a blocking statute[40] 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.[41] 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.[42] On the US 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 was expected in 2020. If presented, 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 is collected in bulk (big data), and the government regulators increasingly use electronic evidence retrieval software to sort it.

Similarly, in the context of investigations and prosecutions in criminal and anti-terrorism 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 should make it easier for judges to require a service provider to retain or produce data stored by it when the data is stored in another EU country. This legislative initiative also feeds the discussions between the United States and the European Union on a new treaty aimed at facilitating cross-border search warrants without going through the international letters rogatory provided for by the Hague Convention.

39 ibid., footnote 37.

40 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.

41 ibid., Article 1 bis.

42 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.

Finally, with regard to civil procedure, the statutory regime defining and specifying the protection of business secrecy enacted 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. For instance, pursuant to the 2018 Act (now in the Commerce Code), the parties to a lawsuit may agree on the scope of information that must remain confidential, following which the judge may limit the disclosure of such information, including within the court's order. This type of solution looks pretty close to what a discovery plan would provide under the US federal rules of evidence.[43]

43 See chapter 10, page 87.

Appendix 1

ABOUT THE AUTHORS

OLIVIER DE COURCEL

Féral-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 areas 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.

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

an LBR business

ISBN 978-1-83862-447-7