THE e-Discovery and Information Governance Law Review

Editor
Tess Blair

THE LawReviews

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.

Appendix 1

ABOUT THE AUTHORS

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.

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

ISBN 978-1-912228-76-8