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 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.

Appendix 1

ABOUT THE AUTHORS

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.

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.

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.

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.

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

ISBN 978-1-912228-76-8