Research Handbook in Data Science and Law

Edited by

Vanessa Mak
*Tilburg University, the Netherlands*

Eric Tjong Tjin Tai
*Tilburg University, the Netherlands*

Anna Berlee
*Utrecht University, the Netherlands*

RESEARCH HANDBOOKS IN INFORMATION LAW

Edward Elgar
Cheltenham, UK • Northampton, MA, USA
© Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee 2018

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical or photocopying, recording, or otherwise without the prior permission of the publisher.

Published by
Edward Elgar Publishing Limited
The Lypiats
15 Lansdown Road
Cheltenham
Glos GL50 2JA
UK

Edward Elgar Publishing, Inc.
William Pratt House
9 Dewey Court
Northampton
Massachusetts 01060
USA

A catalogue record for this book is available from the British Library

Library of Congress Control Number: 2018946029

This book is available electronically in the Elgaronline
Law subject collection
DOI 10.4337/9781788111300

ISBN 978 1 78811 129 4 (cased)
ISBN 978 1 78811 130 0 (eBook)

Typeset by Servis Filmsetting Ltd, Stockport, Cheshire
Printed and bound in Great Britain by TJ International Ltd, Padstow

Contents

List of figures vii
List of tables viii
List of contributors ix

1 Introduction
Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee 1

PART I REGULATING DATA SCIENCE

2 Contract and consumer law
Vanessa Mak 17

3 Liability for data loss
Vincenzo Zeno-Zencovich 39

4 Liability for (semi)autonomous systems: robots and algorithms
Eric Tjong Tjin Tai 55

5 Consumer contracts and the Internet of Things
Katarzyna Kryla-Cudna 83

6 Pledge and attachment of digital data under Belgian law
Koen Swinnen 108

7 Data and intellectual property law
Michael Mattioli 133

8 Legal tech and blockchain for corporate governance and shareholders
Anne Lafarre and Christoph Van der Elst 153

9 Data and competition law
Rupprecht Podszun and Stephan Kreifels 183

10 Data science, data crime and the law
Maria Grazia Porcedda and David S. Wall 214

11 Data-driven regulation and governance in smart cities
Sofia Ranchordás and Abram Klop 245
12 Data science and public administration research: connecting agency rules and red tape
   Wesley Kaufmann
   274

13 Data science and taxation
   Ronald Russo
   304

14 Data localisation measures and their impacts on data science
   Helena Ursic, Ruslan Nurullaev, Michel Ohmedo Cuervas and Pawel Szulewski
   322

PART II DEVELOPING A NEW DISCIPLINE

15 Methods of data research for law
   Bart Custers
   355

16 Data and fundamental rights
   Angela Daly, Anna Carlson and Tess Van Geelen
   378

17 Granular legal norms: big data and the personalization of private law
   Christoph Busch and Alberto De Franceschi
   408

18 Data analysis, artificial intelligence and the judiciary system
   Bart Jan van Ettekoven and Corien Prins
   425

19 Conclusion
   Vanessa Mak, Eric Tjong Tjin Tai and Anna Berlee
   448

Index
   463

Figures

10.1 Types of data in large data sets
   220
10.2 Risk, threat and harm in relation to technology, data and information
   226
12.1 Multidimensional red tape, compliance costs, and administrative burden
   284
15.1 Visual representation of US Supreme Court cases on privacy in Ravellaw
   366
15.2 Visual representation of a sentiment analysis on social media by Coosto
   369
3. Liability for data loss

Vincenzo Zeno-Zencovich*

1. DATASPHERE

Our societies are, already, growingly and irreversibly, data societies. Each year zetabytes (i.e., $1000^7 = 1,000,000,000,000,000,000,000,000$) of data are generated. Once upon a time humans interacting with digital devices were the main sources of data. With the development of the Internet-of-Things (IoT) billions and billions of objects, animals, plants, buildings are already and will be generating, communicating, storing further data, every instant of every day.

All this data will be collected, aggregated, processed. The mainframe computers will generate further data that will be combined with other data, in a never-ending process.

This ‘datasphere’ is not only potentially infinite, but is the digital representation of everything we can digitalize, not only on this planet but in the whole universe (e.g., the data which is sent to us by spacecraft further and further away from the Earth).

An individual, a building, a forest exist in their physical elements. But they exist also as the whole of the data which represent them, and what is even more important, in time, in space and in their relations.

In this context, what do we mean by ‘data loss’? A 19th century dogmatic lawyer would have probably written a whole book on the topic, thoroughly investigating up-stream to the sources of data, and down-stream to their unlimited uses to understand where the lost data have ended up and if any redress is available.

The purpose of this chapter is, decidedly, less ambitious, and much more down-to-earth.

* All the works and texts cited in the footnotes and present on the internet have been accessed between August 1 and October 31, 2017.

2. ‘LOSS’

The first point one should make is what we mean by ‘data loss’. When does this phenomenon become of some significance? To borrow an example from the physical world, we all lose hair — which incidentally contains very revealing data on our DNA — but thank goodness nobody, not even the staunchest supporter of pervasive regulation, has considered it worthy of legal intervention.

And prior to the issue of relevance a civilian asks himself/herself what are the ownership issues. One can ‘lose’ only what one owns. One cannot ‘lose’ the dust on one’s shoes, the insect flying in our room, the shade of our body.2 ‘Ownership’ of data, however, is far from a settled issue.

In the first place, does one ‘own’ one’s own data? ‘Own’, in the sense that one has a property right (in a civilian sense) over such data?3 Or does one have the right to control certain (not all) uses of such data and to prevent them in certain cases? Again a civilian might qualify this as a limited ius arcendi, but not as a fully-fledged property right. Probably it might be more appropriate to use a less engaging term: entitlement.4

Setting aside personal data — in itself a fuzzy notion — does one ‘own’ the data one holds?5 Does one ‘own’ data which — so to speak — are in the public domain: what time it is, the weather, statistical data, etc? When such data is organized might it be protected, in the European Union, by a sui generis right? But if it is not structured? When does one become the ‘owner’ of data? When one generates them (e.g., data on the sales of a firm)? When they are stored in a portion of digital memory to which one has exclusive access?

Entitlement to data becomes a relevant issue — as we shall see — when discussing remedies (mostly damages) for the loss of data.

Further issues arise from the intangible nature of data, which economists generally qualify as ‘public goods’ in the sense that they are not rivalrous and non-consumable. This means not only that many other persons or entities may share the same data, but also that, quite commonly, data are generated by two or more persons who can claim an equal entitlement:6 in a family relation the status of spouse, parent, son, brother, etc. necessarily implies the existence of data pertaining to someone else.7 The parties of a contract (buyer/seller; landlord/tenant; employer/employee) necessarily must share the data concerning their relationship.8

We therefore have data which is intrinsically common to two or more entities. If a bank loses all the data concerning its accounts, it loses also the data related to its clients.

These caveats must be taken into account when analysing the legal implications of data losses.


8 The issue was pioneered by the present European Data Protection Supervisors Giovanni Buttarelli in his Bosco dati e tutela della riservatezza. La privacy nella società dell’informazione, Giuffrè, 1997, p. 194:

Does the law necessarily imply that the use of data be exclusively and necessarily individual, or can one imagine that forms of shared entitlement are allowed between two physical persons who are in a very tight relationship of interests.


9 Not to mention genetic data which can ‘belong’ to several generations: see the Iceland Supreme Court, 7/11.2003, n. 151, Grunmennsóttir v. Iceland (available at https://epic.org/privacy/genetic/icealand_decision.pdf).

10 ‘Shared data’ is a term commonly used in database science and practice; see Scott E. Coull and Erin E. Kenneally, “Toward a Comprehensive Disclosure Control Framework for Shared Data”, IEEE International Conference on Technologies for Homeland Security (November 2013, Boston, MA) available at SSRN: <https://ssrn.com/abstract=2326624> accessed 19 March 2018. In the cases that are presented here, however, data is ‘shared’ because it is ‘common’.
3. CONTRACTUAL REMEDIES

In a considerable amount of cases data are stored in/on digital facilities of third parties with which the entitled person or entity has a contractual relationship.

One is not so much interested in those complex contracts – usually business-to-business – which are the natural development of the outsourcing contracts which were introduced over 30 years ago to enable many businesses to avoid costly investments in computers and related specialized personnel by paying a periodical fee to a digital service provider who not only stores the data but also processed it (typically for pay-rolls, balance sheets, tax forms etc.).

The fact that the computing capacity is multiplied; that the service is rendered often through ‘cloud’ techniques; and that data is collected and forwarded through a multitude of devices, does not seem to change the legal substance of the problem.

Is the service provider liable for the loss of data? This depends on the size of the parties, if they bargain at arm’s length, or if there is significant unbalance in favour of the service provider. In the latter case one can expect widespread use of exemption or limitation clauses similar to those already existing in most outsourcing contracts.

As most of these providers are global operators standard terms will be the same mostly in every country, and no effort will be made to adapt them to the specific jurisdiction.

One can assume that in most cases the entity entitled adopts technical measures (e.g., back-up) to minimize data losses, or buys insurance. And

the same can be said of the service provider. More specifically one can reasonably expect that state-of-the-art diligence implies the implementation by the professional service provider of high-level safety (to avoid losses) and security (to avoid breaches) procedures. One should, however, consider that in some cases contributory negligence of the person or entity which is availing itself of the service could be invoked. Clearly this depends on factual situations: if some part of the computer infrastructure is within the control of the data generator, one might require that the latter ensure safety measures, including back-ups. But if it is using mainframe and software services of the provider (and therefore disposes only of end-user terminals) it is even difficult to imagine how this could be possible.

What deserve more attention are less formalized relations between small businesses and service providers and between common individuals and service providers.

In the first place it would appear that users of on-line services have a contractual relation with the service provider. It is quite immaterial that the small business or the individual does not sign any contract or pay some monetary consideration. Apart from those who believe in the fairy tale that these services ‘are free and will always be’, users generally remunerate the services they receive through the flow of data they provide (the typical

---

12 See Simon Bradshaw, Christopher Millard, Ian Walden, 'Contracts for Cloud: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services', Queen Mary School of Law Legal Studies Research Paper No. 55/2010 (Sept. 2010), available at SSRN: https://ssrn.com/abstract=1662374: 'Our survey found however that most providers not only avoided giving undertakings in respect of data integrity but actually disclaimed liability for it.' (at p. 21). Similar conclusions in Rolf H. Weber, Dominik Nicolaß Stieger, 'Cloud Computing: A cluster of complex liability issues', (2014) 20(1) Web JCLI. One must add that the contractual terms for the 'cloud' are shrouded in the mist, in the sense that they are not available when one accesses the main websites. This fact, in itself, is revealing.
13 One cannot take it for granted that such limitation clauses will be struck down in E2B contracts: see e.g., the decision by The Hague Gerichtshof (28.9.2016) available at https://uitspraken.rechtspraak.nl/document.aspx?id=ECLI:NL:GHDHA:2016:26900 accessed 19 March 2018, which has held a similar clause valid and rejected the claim for damages of the client of the service provider.
15 This statement, however, requires a number of clarifications which are clearly set out by Ruth Janal, 'Fishing for an Agreement: Data Access and the Notion of Contract', in S. Lohse, R. Schulze, D. Suudemayer (eds), Trading Data in the Digital Economy: Legal Concepts and Tools, Hart/Nomos, 2017, 271.
16 This approach has (finally) been accepted by the EU institutions: see the Proposal for a Directive on certain aspects concerning contracts for the supply of digital content: Art. 3 (Scope):
This Directive shall apply to any contract where the supplier supplies digital content to the consumer or undertakes to do so and, in exchange, a price is to be paid or the consumer actively provides counter-performance other than money in the form of personal data or any other data.
It is however challenged in the Opinion of the EDPS of March 14, 2017 (at § 14): 'Personal data cannot be compared to a price, or money. Personal information is related to a fundamental right and cannot be considered as a commodity'. 'One cannot monetise and subject a fundamental right to a simple commercial transaction, even if it is the individual concerned by the data who is a party to the transaction' (§17). For an analysis of the presentation of personal data as valid consideration for the provision of services see Vincenzo Zeno-Zencovich, 'Il diritto alla personalità dopo la legge sulla protezione dei dati personali', in 1997 Studium Iuris 466, 469.
check-test is the growing amount of web-based services which are not provided if the user does not accept cookies.\textsuperscript{17}

Even if the entitled person or entity owns a device (computer, tablet, hand-set) on which the data, apparently, is stored and is available, it is quite common that such data is not – or is not entirely – in the direct and immediate command-and-control of such person or entity,\textsuperscript{18} but in most cases is memorized in an external digital memory accessible on-line. Again the check-test is the availability of such data when there is no internet network connection.

In these cases the relationship between user and service provider are, apparently, regulated by neatly tucked away ‘general terms of service’ which one finds in fine print at the bottom of the home-page of the provider and which, quite normally, are ignored by any sane user. It is worthwhile reproducing some of the relevant provisions on data loss or which is tantamount, on denial of service. It is sufficient to peruse the main providers of search engines or of social media to encounter a flourish of clauses which exclude any sort of liability.

This is how the rule is expressed in Facebook’s terms of service: ‘We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections’.\textsuperscript{19}

\textsuperscript{17} The point has been aptly made by the Italian Competition and Consumer Authority in the WhatsApp II case (11.5.2017). Available at <http://www.agcm.it/component/joomdoc/allegati-news/PS10601_soersanz_omi.pdf?download.html> accessed 19 March 2018.


\textsuperscript{19} Art 15.3 Facebook Statement of Rights and Responsibilities: We try to keep Facebook up, bug-free, and safe, but you use it at your own risk. We are providing Facebook as it is without any express or implied warranties including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, and non-infringement. We do not guarantee that Facebook will always be safe, secure or error-free or that Facebook will always function without disruptions, delays or imperfections. Facebook is not responsible for the actions, content, information, or data of third parties and you release us, our directors, officers, employees, and agents from any claims and damages, known and unknown, arising out of or in any way connected with any claim you have against any such third parties. If you are a California resident, you waive California civil code §1542, which says: A general release does not extend to claims which the creditor does not know or suspect to exist in his or her favor at the time of executing the release, which if known by him or her must have materially affected his or her settlement with the debtor. We will not be liable to you for any lost profits or other consequential, special, indirect, or incidental damages arising out of or in connection with this statement or Facebook, even if we have been advised of the possibility of such damages. Our aggregate liability arising out of this statement or Facebook will not exceed the greater of one hundred dollars ($100) or the amount you have paid us in the past twelve months. Applicable law may not allow the limitation or exclusion of liability or incidental or consequential damages, so the above limitation or exclusion may not apply to you. In such cases, Facebook’s liability will be limited to the fullest extent permitted by applicable law.

Our Warranties and Disclaimers

We provide our Services using a commercially reasonable level of skill and care and we hope that you will enjoy using them. But there are certain things that we do not promise about our Services.

Other than as expressly set out in these terms or additional terms, neither Google nor its suppliers or distributors makes any specific promises about the Services. For example, we do not make any commitments about the content within the Services, the specific functions of the Services or their reliability, availability or ability to meet your needs. We provide the Services ‘as is’.

Some jurisdictions provide for certain warranties, like the implied warranty of merchantability, fitness for a particular purpose and non-infringement. To the extent permitted by law, we exclude all warranties.

Liability for our Services

When permitted by law, Google and its suppliers and distributors will not be responsible for lost profits, revenues or data, financial losses or indirect, special, consequential, exemplary or punitive damages.

To the extent permitted by law, the total liability of Google and its suppliers and distributors for any claims under these terms, including for any implied warranties, is limited to the amount that you paid us to use the Services (or, if we choose, to supplying you with the Services again).

In all cases, Google and its suppliers and distributors will not be liable for any loss or damage that is not reasonably foreseeable.

We recognise that in some countries, you might have legal rights as a consumer. If you are using the Services for a personal purpose, then nothing in these terms or any additional terms limits any consumers’ legal rights which may not be waived by contract.

Business uses of our Services

If you are using our Services on behalf of a business, that business accepts these terms. It will hold harmless and indemnify Google and its affiliates, offic-
Twitter’s terms of service are not dissimilar: ‘The Twitter Entities make no warranty or representation and disclaim all responsibility and liability for (. . .) any harm to your computer system, loss of data, or other harm that results from your access to or use of the Services or any Content.’

Flickr’s terms of service are equally peremptory and relevant, considering the nature of the data (photos) liable to be lost: ‘Your use of Flickr APIs is at your own discretion and risk, and you will be solely responsible for (. . .) any damage to your computer system or loss of data.’

Are these clauses valid? In an EU law perspective they are radically void when they purport to regulate a consumer/professional relationship inasmuch they are in blatant violation of the Unfair Terms Directive, and specifically of its black-list clauses set out in the Annex. Practically all the letters, from a) to q), could be applied to the cited standard terms. It is sufficient here to refer to letter b): ‘Inappropriately excluding or limiting the legal rights of the consumer vis-à-vis the seller or supplier or another party in the event of total or partial non-performance or inadequate performance by the seller or supplier of any of the contractual obligations.’

One can therefore assume that – with all the doubts on evidence and on liquidation of damages which will be seen further on – the service provider is entirely liable for losses due to its professional negligence, unless it can prove typical exonerating circumstances such as force majeure, State intervention, unavoidable events (such as unprecedented and unforeseeable hacking attempts or virus infections).

If provision of data for the digital services rendered is considered an

---

Some of the Flickr APIs may be experimental and not tested in any manner. Flickr does not represent or warrant that any Flickr APIs are free of inaccuracies, errors, bugs, or interruptions, or are reliable, accurate, complete, or otherwise valid. The Flickr APIs are provided ‘as is’ with no warranty, express or implied, of any kind and Flickr expressly disclaims any and all warranties and conditions, including, but not limited to, any implied warranty of merchantability, fitness for a particular purpose, availability, security, title and/or non-infringement. Your use of Flickr APIs is at your own discretion and risk, and you will be solely responsible for any damage that results from the use of any Flickr APIs including, but not limited to, any damage to your computer system or loss of data.

8. Limitation of Liability
Flickr shall not, under any circumstances, be liable to you for any indirect, incidental, consequential, special or exemplary damages arising out of or in connection with use of the Flickr APIs, whether based on breach of contract, breach of warranty, tort (including negligence, product liability or otherwise), or any other pecuniary loss, whether or not Flickr has been advised of the possibility of such damages. Under no circumstances shall Flickr be liable to you for: any amount.

adequate consideration for establishing the existence of a contract at that point it would appear that all the normal rules on performance/non-performance should apply. On the other hand, in ordinary contracts, liability of the receiving party does not change whether it has been paid in cash, precious metal, government bonds, or simply off-setting an existing debt.

What if the user cannot qualify as a ‘consumer’ according to general EU law? In the first place one should note that in the field of telecommunication services EU directives make no difference between the statuses of users. This means that rights and guarantees vis-à-vis the telecom operator apply to both ‘consumers’ and ‘non-consumers’ (typically enterprises). Clearly this is an express normative provision, but the result is that telecom operators are burdened by a higher level of liability than over-the-top (OTT) service providers.

If this is a remark de lege ferenda, de lege lata one has to investigate jurisdiction by jurisdiction – if the exonerating clauses are valid towards non-consumer users. In some jurisdictions, clauses which limit liability require a specific form to be valid (written, express approval, etc.). In other jurisdictions – mostly of common law – one could apply the broad and never clearly defined notion of unconscionability. At any rate, at the end of the day, it will be up to the courts to decide whether such clauses are to be considered valid or void, and an academic lawyer’s imagination is positively shallow if compared with that of judges.

4. NON-CONTRACTUAL REMEDIES

The ways in which a loss of data may fall outside the scope of a contractual relation are countless: a careless act makes a hand-set fall in the deep blue sea; a sudden interruption of electric power (like in the classical ‘cable cases’) destroys a file while one is working on it; a virus infection transfers an unsuspecting third party prevents access to a database. One can assume that there has been negligence and that the result is the definite and non-reparable loss of data. Here the initial problems will arise. In a civil context are data an asset that belongs to the person’s patrimony? Does the person who has suffered the damage hold a recognized right over such data, or does he/she simply have a right to use the data and to prevent others from using them?

Extra-contractual remedies generally protect property from negligent damage brought by third parties. But, again, is data ‘property’? Once, on the basis of arguments that here are shared, one has excluded this approach, must one necessarily come to the conclusion that loss of data is simply one of the many cases of pure economic loss, and therefore does
not give rise to compensation? Again the answer depends on how the case is presented: clearly, if the claim is that loss of data has brought business activities to a stand-still, the previously cited ‘cable-cases’ will apply. But if the damage is related to some essential, albeit immaterial, component of the business activity, which hypothetically might even be a valuable asset in the balance sheet, one could imagine to extend to the lost database the protection already granted to other non-tangible assets such as goodwill or credit-worthiness.

There are many indicia that suggest that loss of data could be considered akin to the destruction of any valuable asset in the possession of the damaged party. The first and foremost is that wilful destruction of data is, according to the Budapest Convention, a crime. This allows the inference that data are a protected entity, and therefore that negligent acts – which determine the loss of data – should be subject to civil liability.

The second element that should be considered is that if personal data are qualified – as mainstream legal doctrine holds in many continental legal systems – as personality rights there is no reason to afford them less protection than other intangible situations (name, image, reputation, etc.). And even if personal data is not qualified as a personality right, it is a fundamental right under article 8 of the European Charter of Fundamental Rights.

Again it will be up to the courts – which in continental Europe and in the US (but not in the UK) have always made an expansive use of extra-contractual liability as the means to establish ‘new’ rights (literally, remedies have preceded rights). However, at this stage it is still unclear what the arguments for and the consequences of civil liability for the loss of data (or for the loss of access to data) will be.

5. THE CASE OF LOSS OF PERSONAL DATA

One must consider that among the most common cases of data losses there are, and will be, the loss of personal data. The topic is amply considered in the General Data Protection Regulation which applies from May 2018 onwards.

The GDPR qualifies data loss as personal data breach which entails liability on behalf of the controller or processor who is burdened with an obligation to ensure an appropriate level of security, to inform the data subject (article 34) and to make good the person who has suffered damage.

From a practical point one can easily imagine that natural persons will prefer to bring their claim on the basis of such explicit norms, rather than engaging in academic qualifications on the notion of data and of their legal relevance. In such a manner also the loss of data which, in abstracto, could be considered not to be ‘personal data’ (typically when an individual collects statistics, news reports, data and information in the public domain that do not concern him/herself), will be encompassed in the GDPR provisions.

As the GDPR protects natural persons this leaves open the issue of the loss of data which ‘belong’ to a legal entity.

---

36 Art 4 (Definitions), n: 12: “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
37 Art 32 (Security of processing)
2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.
38 Art 82 (Right to compensation and liability)
1. Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
2. Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where he has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
6. EVIDENCE

Anybody familiar with the case-law in liability for loss of valuable objects deposited in a bank’s vault or in the hotel safe is aware of the difficulty of providing evidence of what was actually lost (generally, stolen). The depositor fears that the depositor is adding into the list of stolen items objects that were never actually deposited. Both parties face a probatio diabolica: should the depositor have kept a register, with witnesses of what he/she deposited? Should the depositor be able to confirm that what has been declared is truthful?

This dilemma – which is generally solved through burden-of-proof rules – presents itself paradoxically when it comes to data losses. If one had to prove what data has actually been lost, that data would be in the availability of the owner, and therefore there would be no loss. To prove that the manuscrip of the volume Research Handbook in Data Science and Law has been lost as a result of the negligence of the digital service provider or of a third party, can one limit oneself to indicate, if the log book is accessible, the number of bytes the file contained? When a business loses thousands of contacts how can it prove how many they were, how updated they were, the frequency of exchange with each contact, etc.? And the bigger the database that has been lost, the more complex is the reconstruction of its precise features: what exactly did it contain? How many entities were included? What is the nature of the meta-data?

7. QUANTUM OF DAMAGES

Although we live in a world dominated by data, in which data are considered an essential element of economy and of wealth (the ‘new oil’ according to certain rhetorical literature) it is still quite uncertain what the actual value of data is, and if in reality the wealth is not in the (big) data itself, but rather in the computational tools (data analytics) used to extract valuable information from it. One has precise market prices for profiles of individuals used for marketing (especially in the medical sector), but very little evidence on how much a database of clients is worth in a business transaction, or what is the overall cost to rebuild a lost directory. If this is valid for business entities, even more difficulties can be encountered when the loss concerns personal correspondence, addresses, photographs, videos. How to evaluate the damage from the loss of hundreds of love messages, an archive of family snap-shots, etc.? One can imagine applying rule-of-thumb criteria common for non-patrimonial losses, but this leaves a very wide area of discretion, in which the position of the defendant service provider is greatly advantaged in the countries (i.e., all, except the US) where no punitive damages are awarded.

---


42 The typical English response is that there is no evidence: see Andre Anor v Clydesdale Bank Plc [2013] EWHC 169 (Ch). At the opposite the Italian Corte di Cassazione states that one can prove the consent through simple presumptions and witnesses: see for the latest in long line of decisions Cassazione civile, sez. 1, 27.7.2017, n. 18637.

This reasonable forecast suggests that from a policy perspective compensation schemes should be introduced. One can easily expect that in most cases the data loss will be a ‘mass loss’, in the sense that some break-down of the system or some external breach will determine the loss of data pertaining to hundreds, thousands or even millions of individuals or entities.

In these cases ordinary judicial remedies (both contractual and non-contractual) are quite ineffective also because of the very high administrative and legal costs.

Much more efficient – de lege ferenda – is a system in which compulsory insurance for data service providers is supplemented by simplified and semi-automatic compensation procedures, similar – although on a larger scale – to those one already finds in the EU transport law for the protection of passengers.⁴⁵

To conclude: data losses, as many other aspects concerning data societies and data economies, still lie in uncharted waters. The notion itself of data and its legal classification is debatable, at least among jurists. But also other sciences – noticeably economic – do not yet provide certain and agreed bearings. Only the combined efforts of academic research, advised regulators and competent courts can slowly open the way to a more precise and reliable setting.