PRAVNI ZAPISI, God. XIV, br. 2 (2023)

UDK 347.736:342.721
DOI 10.5937/pravzap0-46513

ORIGINAL SCIENTIFIC ARTICLE

ČLANCI / ARTICLES

*Tibor Tajti (Thaythy)**

A NEW FRONTIER: THE CHALLENGES SURROUNDING THE DEEPENING IMPACT OF DATA PROTECTION REGULATIONS ON BANKRUPTCY LAW

> *"Admittedly, neither customer databases nor privacy concerns are new. What is new is the greatly expanded scope of data collection and an e-commerce environment where customer information is regarded as core asset. These new dynamics, combined with increasing public awareness of online privacy issues, have created new privacy concerns for bankruptcy. There is no satisfactory answer to be found in the current law."*
>
> **Michael Geist****

Abstract: *Notwithstanding the unprecedented and global prestige that data privacy (or data protection, in Europe) law has gained in the 21st century, comparative analyses of the effects flowing from the intensifying impact of data protection law on bankruptcy (insolvency) law remain unexplored. In addition to canvassing the history and contours of the data protection–bankruptcy law interface, through an empirical comparison of available court and data protection agency (authority) cases in multiple jurisdictions, this article fills this gap by identifying and exemplifying various modalities through which data protection law interferes with the bankruptcy process or creates tensions between the two branches of law, based on the comparison of available court and data protection authority (agency) cases in Europe (including the United Kingdom), the United States, as well as Canada and China, as middle-ground systems.*

Key words: Bankruptcy (Insolvency) Law, Data Protection (Privacy), Recast EU Insolvency Regulation 2015/848, European e-Justice Portal, Interconnected Insolvency Registries, Red Tape, Middle-Ground Systems.

* Professor of Law, Central European University – Private University, Vienna; e-mail: tajtit@ceu.edu

The author extends his gratitude to Joshua Haynes-Mannering for his linguistic assistance and Ágnes Horváth for her research assistance (both doctoral candidates).

** Geist, M., 2020, When Dot-Coms Die: The E-Commerce Challenge to Canada's Bankruptcy Law, *Canadian Business Law Journal*, 37, p. 70.

1. Introduction

Notwithstanding the unprecedented and global prestige that data privacy (or data protection, in Europe) law has gained in the 21st century, comparative analyses of the effects stemming from the increasing impact of data protection law on bankruptcy law remain unexplored. Consequently, this article's central aim is to show that the various forms in which data protection law is impacting bankruptcy law are intensifying, in the sense that these branches of law are colliding in more and more instances, either because of the irreconcilable policy goals or because of the amount of red tape that data protection regulations are imposing. The intensity of changes has reached the point where the problems that this generates require regulatory reactions in lieu of the hereinbefore ad hoc solutions of courts and governmental agencies (authorities).

The multiplying amount of reported, and the increase in the number of commented cases touching upon this interface, suggests that growing attention is being devoted to the central issue that is the focus here. Notwithstanding this, while in the US some modest regulatory efforts have already been made to enhance privacy right protections in the context of bankruptcy proceedings, in Europe, the General Data Protection Regulation (GDPR) – the most comprehensive data protection regulation globally – contains no bankruptcy-specific provisions whatsoever. What Europe has, however, are hard cases justifying the legitimacy of this paper and the claims made herein. It will suffice to mention the United Kingdom (UK) 2013 *Southern Pacific* case,[1] where the application of data privacy laws burdened insolvency practitioners with expensive red tape or an Italian one where creditors saw their insolvency recovery plans frustrated due to the indisposability of genetic data as a particular class of property in insolvency proceedings (the Italian *Ogliastra* region case).[2]

As the comprehension of the myriad of questions regarding the data protection–bankruptcy interface requires in-depth knowledge of both areas, canvassing both areas is inevitable. Moreover, as data protection is based on constitutional and partly also on human rights law on both sides of the Atlantic, it is necessary to briefly reflect also on the known and potential impacts of these branches of law on bankruptcy law. As will be

1 *Re Southern Pacific Personal Loans Ltd.,* [2013] EWHC 2485 (Ch).

2 The synopsis of the case is based on Piciocchi, C. *et al*., 2018, Legal Issue in Governing Genetic Biobanks: The Italian Framework as a Case Study for the Implications for Citizen's Health through Public-Private Initiatives, *Journal of Community Genetics*, Vol. 9, Issue 2, pp. 177, 181.

seen, while in Europe there are already a few relatively recent vintage cases implicating the interface adjudicated based on the constitutional law of the European Union (EU), or Council of Europe human rights law, such cases have almost routinely been decided upon based on free speech rights in the United States (US) for decades.

The US caseload is informative not only because of the heightened emphasis on free speech concerns (as a rule that creates a balance benefitting the needs of bankruptcy law more than in Europe), but also because problems common with Europe and the rest of the globe also emerge increasingly, the sale of bulk personal data in bankruptcy proceedings being the best example. This does prove that each of these jurisdictions has what to offer for better understanding of the interface, as corroborated also by the recent experiences of middle-ground systems such as Canada and China – which is touched upon briefly as well.

Considering the above, following an introduction on the differing nomenclatures of EU and the US, and the connected philosophical underpinnings, comes an outline of their bankruptcy and data privacy laws, before the case analyses. The pivotal importance attributed to case law is justified not only with their empirical value, its capability to unearth real problems often previously unseen, but also because of a desire to forge a seminal catalogue of the modalities, whereby data protection impacts bankruptcy law – ranging from "happy co-existence" to colliding cases, as well as cases requiring courts to balance the priorities of the two branches of law.

2. The Differing Nomenclatures and Underlying Philosophies on the Two Sides of the Atlantic

Lee Bygrave, a leading authority on contemporary data protection law, warned that although "[t]he issue of nomenclature might be dismissed as trivial since it primarily relates to 'packaging' ... the packaging sends important signals about the law's remit, particularly to newcomers."[3] This applies *a fortiori* in emerging areas such as the interface between data protection and bankruptcy law, especially if this area is considered comparatively. The terminology-related intermezzo below is intended to act as a compass for the ensuing multi-disciplinary discussion, which touches on bankruptcy, data protection (privacy), and tenets from constitutional and human rights law.

3 Bygrave, L., 2014, *Data Privacy Law*, Oxford, OUP, p. 23.

2.1. BANKRUPTCY OR INSOLVENCY LAW? – DIFFERING NOMENCLATURES ON THE TWO SIDES OF THE ATLANTIC

For our purposes, the radically different breadth of the cardinal terms "bankruptcy" and "insolvency", on the two sides of the Atlantic, ought to be demarcated. To wit, while *bankruptcy* for US lawyers extends to all known types of statutory proceedings enshrined in the Bankruptcy Code and other linked sources of law, *insolvency* is used solely in reference to "[t]he condition of being unable to pay debts as they fall due or in the usual course of business."[4] Today, in the US, insolvency is a precondition for filing a petition to open bankruptcy proceedings with a bankruptcy court solely under Chapter 9 of the US Bankruptcy Code, which governs municipal bankruptcy cases.[5] It is worth mentioning that according to US legal historians, "insolvency law ... was [initially] conceived as a debtor relief law, and could be commenced by the impoverished *individual* debtor".[6]

In the UK, on the other hand, *insolvency law* is "a distinct regime"[7] applicable only to companies "when a company is within formal insolvency proceedings."[8] Roy Goode, the doyen of English commercial law, therefore speaks of "corporate insolvency law."[9] While *insolvency* therefore has broader meaning in the UK (and in other jurisdictions which have adopted the British nomenclature, including the EU) than in the US, the term *bankruptcy* is much narrower, as it applies only to formal statutory proceedings against individuals.[10] As UK bankruptcy law's ultimate objective is to "discharge the bankrupt [individual] from his liabilities,"[11] it is equivalent to US Chapter 7 bankruptcies.[12]

4 Garner, B. A. (ed.), 2009, *Black's Law Dictionary*, Deluxe 9th ed. Eagan, West.

5 See § 109(c)(3) of the Bankruptcy Code. Other additional requirements apply to municipalities which are defined as a "political subdivision or public agency or instrumentality of state", such as cities under § 101(40) because "the special sovereignty interests of the state." Tabb, J. C., 2020, *The Law of Bankruptcy*, 5th ed., St. Paul, West Academic, § 2.2, p. 124.

6 Noel, R. F., 1919, *History of Bankruptcy Law*, Washington, D. C., Chas. H. Potter & Co, pp. 10–11. Cited in Tabb, J. C., 2020, p. 2, note 7, (emphasis by author).

7 Goode, R., McKendrick, E., 2020, *Goode and McKendrick on Commercial Law*, 6th ed., London, Penguin, pp. 923 ff.

8 Gullifer, L., Payne, J., 2020, *Corporate Finance Law – Principles and Policy*, 3rd ed., Oxford, Hart, p. 98.

9 Goode, R., McKendrick, E., 2020, p. 924.

10 See Insolvency Act 1986, UK Public General Acts, 1986 c. 45, Part IX, Chapter I, Section 264(1), reading that bankruptcy proceedings start with the filing of "[a] petition for a bankruptcy order ... against an individual."

11 Goode, R., McKendrick, E., 2020, p. 927.

12 Similarly, Part 7A on 'Debt relief orders' and Part VIII ('Individual voluntary arrangements') of the UK Insolvency Act 1986 may be taken as the UK counterpart to Chapter 13 of the US Bankruptcy Code.

This terminological disparity between the two sides of the Atlantic is of relevance for us here because EU law is primarily influenced by English nomenclature, though the exact connotation of the nomenclature in relevant EU legislation is fixed by the legislation itself. For example, the Recast Insolvency Regulation 2015/848[13] – the regulation at the very center of our observations – applies to companies, self-employed persons, and even to consumer-debtors,[14] demonstrating that EU law's usage of the term "bankruptcy law" is not exactly coextensive with the US's nor with the UK's.

US terminology is favored herein, save when topics from the EU, UK or other jurisdictions utilizing a differing nomenclature are being referred to. In the case of the latter, the local nomenclature is used. In English language publications and in official and unofficial translations of the national bankruptcy acts of EU member states that do not use English as their official language, EU and English nomenclature seems to be dominant, though often the selection of terms depends on the background and preferences of the translators.

One last related point must be made. Namely, the distinctions drawn above between proceedings against individuals (consumers) and legal entities (companies) may give the mistaken impression that data protection laws protect only bankrupt *individual debtors* in "bankruptcy proceedings" and that this article deals exclusively with such scenarios. On the contrary, although the protection of EU data protection laws is, indeed, limited to "natural persons", there is also a need to protect the data concerning natural persons appearing in various roles in insolvency proceedings conducted against juridical entities. Namely, individuals whom European data protection law is designed to protect may appear as individual debtors not exercising an independent business or professional activity, individual-debtors exercising such activities, individual-creditors, and individuals serving as insolvency practitioners,[15] or ancillary service-providers like US examiners.[16]

13 European Insolvency Regulation (EIR), Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (recast).

14 Recast European Insolvency Regulation, recitals 9–10, the first of which states that "[t]he scope of this Regulation should apply to insolvency proceedings which meet the conditions set out in it, *irrespective of whether the debtor is a natural person or a legal person, a trader or an individual*," (emphasis by author).

15 EIR Art. 2(5) defines insolvency practitioners as "any person or body."

16 Examiners may be appointed by bankruptcy courts pursuant to §1104(c) of the US Bankruptcy Code to investigate the debtor's affairs "including an investigation of any allegations of fraud, dishonesty, incompetence, misconduct, mismanagement, or irregularity in the management of the affairs of the debtor of by current or former

2.2. DATA PROTECTION VERSUS DATA PRIVACY LAW

In Europe, the expression "data protection law" has become the dominant term for this burgeoning area of law. This designation is a calque of the German term *Datenschutz.*[17] Some European scholars nonetheless prefer the term "data privacy", which is the established designation in the US. While both terms may be used interchangeably, the latter has a broader semantic scope. This difference stems primarily from the fact that EU *data protection* law has been consolidated into a distinct, clearly identifiable branch of law with the General Data Protection Regulation (GDPR) as the heart of the entire regime. What is covered by the GDPR, in other words, is European data protection law.

As opposed to the EU, US privacy laws are scattered across different areas of the legal system, sometimes dressed as constitutional doctrine and elsewhere as narrow, sector-specific statutes, ranging from the broader Privacy Act 1974 introducing the Code of Fair Information Practices[18] for federal agencies, to the sector-specific Children's Online Private Protection Act of 1998. Although criticized for its myopic approach, the US practice of introducing narrow and tailormade sector-specific solutions piecemeal may prove capable of tackling the idiosyncratic data protection problems of the sector(s) regulated by the statute in question and simultaneously avoiding unintended systemic consequences better than generalist systems, like the GDPR, could realistically hope to.

There is, however, a much more fundamental difference between the two sides of the Atlantic; namely, they traditionally hold "widely differing views on data privacy",[19] which have been characterized by some as no

management of the debtor." See also the case *Maxwell Communication Corp. v. Sociètè Gènèrale* 93 F.3d 1036 (US Court of Appeals, 2nd Cir., 1996).

17 Bygrave, L., 2014, p. 58.

18 See the succinct reference to the 1974 Privacy Act on the website of the Office of Privacy and Civil Liberties of the U.S. Department of Justice (https://www.justice.gov/opcl/privacy-act-1974, 6 September 2023).

19 Bennett, S. C., 2012, The "Right to Be Forgotten": Reconciling EU and US Perspectives, *Berkeley Journal of International Law*, Vol. 30, Issue 1, p. 161, p. 168, n. 25 citing also Levin, A., Nicholson, J. M., 2005, Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground, *University of Ottawa Law & Technology Journal*, Vol. 2, No. 2, p. 357, (characterizing the Canadian model as a conceptual middle ground between the EU and the US); Baumer, D. L., Earp, J. B., Poindexter, J.C., 2004, Internet Privacy Law: A Comparison between the United States and the European Union, *Computers & Security*, Vol. 23, Issue 5, pp. 400, 411, (stating the "Compared with the EU ... there is far less legal protection of online privacy in the US."); Salbu, S. R., 2002, The European Union Data Privacy Directive and International Relations, *Vanderbilt Journal of Transnational Law*, Vol. 35, Issue 2, p. 655, (describing first generation EU data protection law as 'aggressive' protector of its values).

less than a "trans-Atlantic privacy clash."[20] Although initially both sides followed an "internationally agreed-upon set of principles"[21] as embodied in the 1980 Privacy Guidelines of the Organization for Economic Co-operation and Development (OECD),[22] subsequent development gradually[23] led to significant divergence between the two. In particular, the Council of Europe's Convention 108[24] (last amended in 2018)[25] introduced standards that were not only more stringent than the OECD Guidelines but whose application was mandatory. No such steps were taken in the US. These European protections were further strengthened when the EU Commission requested that Member States ratify Convention 108, a step that eventually led to data protection becoming a fundamental right.[26] The outcome of this long process is that today, the EU Charter of Fundamental Rights (which gained binding legal force in 2009) and the general principles of EU law ("a body of legal principles, including human rights") rank as primary EU legal norms, coequal with the ones in EU's founding Treaties.[27]

Data privacy law is therefore also a constitutional rights issue in both Europe and the US, though cast in different conceptual forms with given different degrees of protection. In the US, privacy rights in general are somewhat deprioritized due to a traditional "[emphasis on] freedom of ex-

20 Reidenberg, J. R., 2001, E-Commerce and Trans-Atlantic Privacy, *Houston Law Review*, 38, pp. 717, 718.

21 OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188 (2022), p. 3. For further details see Pernot-Leplay, E., 2020, China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law & International Affairs*, Vol. 8, No. 1, pp. 49, 56 ff.

22 OECD, Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), as updated in 2013.

23 In particular, "the underlying substantive ideology of privacy protection," as enshrined in the 1973 US Code of Fair Information Practices, was similar to the EU's fundamental principles because the US had adopted the OECD Guidelines (signed in 1980, ratified in 1998 at the Ottawa OECD Conference). See Boyd, V., 2006, Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization, *Berkeley Journal of International Law*, Vol. 24, Issue 3, p. 939, pp. 943–944. Further, the US Federal Trade Commission formulated a set of "core principles" in 1998, with "notice" having been identified as the "most fundamental principle". *Ibid.*, p. 944.

24 Council of Europe Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108.

25 CETS No. 223, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 10 October 2018).

26 Charter of Fundamental Rights of the European Union, 2012/C 326/02, Article 8, Title II Freedoms ("everyone has the right to the protection of personal data").

27 Craig, P., Búrca, G. de, 2020, *EU Law – Text, Cases, and Materials*, 7th UK ed., Oxford, OUP.

pression over privacy, as a fundamental value."[28] Indeed, numerous cases in which the protection of data privacy was sought by litigants have been overruled on the basis of First Amendment concerns.[29] A shorthand yet apposite description of the differences between the core philosophies of data privacy law in the EU and US, written by James Q. Whitman in 2004, remains basically valid today: while in the US "anxieties and ideals focus principally on the police and other officials, and around the ambition 'to secure the blessings of liberty,' ... on the Continent they focus on the ambition to guarantee everyone's position in society, to guarantee everyone's 'honor'."[30]

Similarities between the two systems exist, nonetheless. The US Fair Credit Reporting Act (1970), for example, imposes the duty on credit reporting agencies to make their records available to the subjects of said records and introduces procedures for correcting such data. Identical responsibilities for data processors are enshrined into the GDPR, although as basic principles.

Some US scholars have been quite critical of the US's sectoral regulatory system. For example, Priscilla M. Regan claimed that "[a]lmost all analyses of privacy protection in the United States conclude that privacy protection is weak, proceeds on a sector-by-sector basis, and consists of a patchwork of protections."[31] Data privacy laws were thus rightly depicted as consisting of a "'reactive' array of state and federal statutes and common law doctrines."

To avoid being accused of not seeing the forest for the trees, the hectic history of EU–US relations concerning the flow of personal data from Europe to the US should not be forgotten either, and in particular, the position of US social-media companies, such as Facebook and Google. This rather non-reciprocal process has also shaped the unequal attitude to data privacy and the differing policy responses of the US and EU. On a macro level, this inevitably leaves imprints on the area, but it does not necessarily affect the concrete outcomes of court and DPA cases. In other words, while the economic and political dimensions of data protection systems radically differ on the opposite sides of the Atlantic, at the micro-level of the novel issues touched upon by the cases discussed below, commonalities can easily be found, and these broader geopolitical issues might be of

28 Bennett, S. C., 2012, p. 168.

29 *Ibid.*, p. 168, notes 36, 37.

30 Whitman, J. Q., 2004, The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Law Journal*, Vol. 113, No. 6, pp. 1151–1222.

31 Regan, P. M., The United States, in: Rule, J. B., Greenleaf, G. (eds.), 2008, *Global Privacy Protection*, Cheltenham, Elgar, p. 52.

lesser relevance. One may thus legitimately wonder, facing a freshly discovered issue, whether differing answers should be given to the tracking of individual internet activity even after users have switched to "incognito mode" on Google?

3. The European Perspectives

3.1. THE "SINGLE MOST IMPACTFUL DATA PRIVACY LAW WORLDWIDE"

For the EU, both insolvency and data protection laws are of high importance.[32] Yet it is fair to claim that the importance of the latter has skyrocketed in Europe due to the increasing impact of new technologies on both consumers and businesses. New technologies make data subjects increasingly "vulnerable" due to the expanded geographical reach of data and the ease with which their personal data can be accessed, processed, and thus also abused. A number of European cases have demonstrated this priority, and indeed, the comprehensive data protection regulatory system enjoys widespread legitimacy, with the GDPR being hailed at the time of its passage as "the single most impactful data privacy law worldwide."[33] The validity of this statement has persisted up until today, although the emergence of middle-ground systems readily proves not only that not all building blocks of the European model are transplantable without often significant adaptations, but also that one should increasingly reckon with the presence of rival models, too.[34]

32 See, in particular, Recitals 3–5 of the EIR, which stresses that the regulation of cross-border insolvencies is a precondition for the proper functioning of the EU's internal market. Recitals 83 and 84, on the other hand, proclaim the goal of promoting the protection of personal data.

33 Cunningham, M., 2013, Diminishing Sovereignty: How European Privacy Law Became International Norm, *Santa Clara Journal of International Law*, 11, p. 430, referring to Shaffer, G., 2000, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, *Yale Journal of International Law,* Vol. 25, pp. 55–88, and Moshell, R., 2005, ... And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection, *Texas Tech Law Review,* 37, pp. 357, 384.

34 See Greenleaf, G., Cottier, B., 2020, 2020 Ends a Decade of 62 New Data Privacy Laws, *Privacy Laws & Business International Report*, 163, pp. 24–26. In Africa, new laws of Kenya and Uganda have been influenced by the GDPR, but only to a limited extent. Interestingly, the three Central Asian countries that passed data privacy laws most recently (specifically, Tajikistan, Uzbekistan and Turkmenistan) did not follow the GDPR model. *Ibid.*, p. 5.

3.2. EUROPEAN INSOLVENCY LAW: MAIN MILESTONES

Unlike the data protection law, EU insolvency law's domain has always been limited, since consensus was only reached on two major programmatic agenda items. These are the coordination of and fostering of cooperation in cross-border insolvency proceedings, and the domestication of the second chance (or fresh start) bankruptcy philosophy. While the first policy was materialized in the European Insolvency Regulation of 29 May 2000 (as recast in 2015),[35] the second culminated recently in the enactment of the 2019 Preventive Restructuring Directive,[36] which was preceded by soft law instruments containing similar content.[37]

Political considerations prevented the EU from advancing further on this front by passing a common European insolvency code containing "substantive" bankruptcy law. Different European countries therefore uphold insolvency law policies and rules that diverge significantly, which remains a concern for the internal market, especially insofar as these divergent approaches concern politically sensitive issues such as the priority and protections afforded to labor (employees) and those afforded to financiers (secured creditors). The 2022 "Proposal for harmonising certain aspects of insolvency law" illustrates these inherent tensions, which are an obstacle to the development of EU capital markets.[38] Notably, this proposal stresses the need to ensure "enhanced transparency for creditors on the

35 Council Regulation (EC) No. 1346/2000 of 29 May 2000 on Insolvency Proceedings, recast by Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings.

36 Directive (EU) 2019/1023 of the European Parliament and of the Council of 20 June 2019 on preventive restructuring frameworks, on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132 (Directive on restructuring and insolvency), *Official Journal Legislation (OJ L)* 172, 26 June 2019, pp. 18–55. The Directive was influenced by US Chapter 11 (Reorganizations) and the rich repository of reorganizations and out-of-court workouts related to US experiences.

37 A Commission communication of 1 October 2004, Community guidelines on State aid for rescuing and restructuring firms in difficulty (*Official Journal* 244, 1 October 2004, pp. 2–17); Commission communication of 5 October 2007, Overcoming the stigma of business failure – for a second chance policy – Implementing the Lisbon Partnership for Growth and Jobs (COM/2007/0584 final); Commission Communication of 25 June 2008, "Think Small First" – A Small Business Act for Europe (COM, 2008, 394 final), and Commission Recommendation of 12 March 2014 on a new approach to business failure and insolvency (L 74/65).

38 Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law, Brussels, 7 December 2022 COM(2022) 702 final 2022/0408 (COD).

key features of national insolvency regimes, including on the rules governing insolvency triggers and the ranking of claims,"[39] objectives which directly contradict those of data protection law policies.

Given the coordination mandate, the first European Insolvency Regulation of 29 May 2000,[40] just like the 2015 Recast in force today,[41] are consequently full of conflict of laws type provisions. Their ultimate effect is thus limited to ensuring that bankruptcy proceedings against the same debtor, opened simultaneously in several member states, can be coordinated efficiently[42] by ensuring that cross-border cases are resolved "in a single set of proceedings, opened in one Member State but effective in others."[43] This objective is achieved through a hierarchical system[44] whereby the main and secondary (ancillary) proceedings use the concept of Centre of Main Interest (COMI)[45] as a tool for deciding which jurisdiction's insolvency proceedings is given priority and thus plays the decisive role – a formula known also to the provisions of US Bankruptcy Code Chapter 15.[46]

3.3. EUROPEAN DATA PROTECTION LAW: MAIN MILESTONES

The short history of Europe data protection began (one could say "modestly") with the passage of the generally applicable Data Protection Directive 95/46/EU (DPD),[47] and somewhat later with its "twin", Regula-

39 Quoted from the European Commission's 2022 Proposal for a Directive harmonising certain aspects of insolvency law (https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/civil-justice/civil-and-commercial-law/insolvency-proceedings_en, 5. 1. 2023).

40 Council Regulation (EC) No. 1346/2000 of 29 May 2000 on insolvency proceedings, *OJ L* 160/1, 30 June 2000.

41 Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings *OJ L* 141, 5 June 2015, pp. 19–72.

42 The coordination of secondary proceedings presumes the requirement for insolvency practitioners to cooperate and communicate with each other in these proceedings (Art. 41 Recast EIR). Bork, R., Zwieten, K. van, 2022, *Commentary on the European Insolvency Regulation*, 2nd ed., Oxford, OUP, para 0.43, p. 38.

43 *Ibid.*, para 0.01, p. 1.

44 This hierarchy is limited in the sense that secondary proceedings are subordinated to main proceedings only in some circumstances: "principally by enabling the insolvency practitioner, in main proceedings, to secure a stay of the realization of assets in secondary proceedings [Art. 33 Recast EIR]." *Ibid.*, para 0.43, p. 38.

45 Compare Section 1502(4) of the US Bankruptcy Code and the more detailed Article 3 of the EU Recast Insolvency Regulation.

46 Section 1502(4) of the US Bankruptcy Code speaks of "foreign main proceeding" and 1502(5) of "foreign non-main proceeding".

47 Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.

tion 45/2001, which was of limited application, governing only personal data processing by the EU Commission.[48] The latter mimicked the former, and is thus of limited importance to this discussion.

This was followed by a rapid expansion of data protection law through several major cases, which unearthed newer problems and revamped parts of the legal framework within an unprecedentedly short period of time, all with the aim of strengthening the protection of privacy. No better examples can be mentioned than the *Google Spain* case,[49] which led to the birth of the *right to be forgotten* – or the right to erasure, in Article 17 of GDPR. The 2014 *Schrems I*[50] and the 2020 *Schrems II*[51] decisions of the CJEU successfully attacked and dismantled the regulatory regimes that purported to ensure the protection of personal data streams flowing from Europe to the US. These and other milestone cases paved the way for the expanded and consolidated regime that was enshrined in the General Data Protection Regulation 2016/679 (GDPR),[52] in force since 25 May 2018, which repealed and replaced its predecessor – unlike the EIR, which "built upon, rather than dismantled, the regulatory framework established by [its predecessor]."[53]

As far as the most recent developments are concerned, the work on the e-Privacy Regulation proposal should be noted. If enacted, this Regulation will replace e-Privacy Directive 2002/58/EC,[54] which regulates electronic communications services (e.g., Skype, WhatsApp, SMS services, fixed and mobile telephone services, cookies, etc.).[55]

48 Regulation (EU) 45/2001 was repealed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No. 1247/2002/EC, *OJ L* 295, 21 November 2018.

49 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos [es], Mario Costeja González* (C 131/12) ECLI:EU:C:2014:317.

50 Schrems I CJEU Case C-362/14.

51 Schrems II CJEU Case C-311/18 (as of 16 July 2020).

52 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) (Text with EEA relevance) *OJ L* 119, 4 May 2016, pp. 1–88.

53 Bork, R., Zwieten, K. van, 2022, p. 2.

54 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 *OJ* (L 201) 37 (E-Privacy Directive), as amended by the EU telecoms reform package from November 2009.

55 See the related data on the EU's Legislative Train Schedule (https://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform, 7. 9. 2023).

Lastly, another subtle point of distinction should be pointed out. Namely, while the first EU insolvency-related piece of legislation took the form of a regulation, data protection law was set out "only" as a directive in the first phase of development. This is telling of the initial perception of the risks of data protection, because regulations are by definition directly applicable in all Member States,[56] while directives "do not have to be addressed to all Member States, and they are binding as to the end to be achieved while leaving some choice as to form and method to the Member States."[57] In other words, the consensus that data protection concerns require not only strict but also common European responses was reached with a delay of more than a decade.

However, given the pressing risks to personal data posed by new technologies, the EU's stance on data protection law has changed within an unprecedentedly short period of time because data protection law also became directly applicable with the GDPR's entrance into force on 15 May 2018. In short, today the Member States' maneuvering room in the data protection domain has shrunk significantly. Counterintuitively, the interpretative powers of Data Protection Authorities (DPAs) – which are national-level bodies – have increased at the same pace, partially due to the plethora of new issues requiring fast answers that have popped up during the GDPR rollout. A US litigant entangled in European (national or cross-border) insolvency proceedings or in a dispute involving data protection laws should therefore not be surprised that clarificatory answers may be provided by the office of a DPA and – irrespective of the GDPR's direct applicability – that these answers may differ from state to state.

3.4. THE NEW ERA: A PARTIAL ACKNOWLEDGEMENT OF THE IMPORTANCE OF THE BANKRUPTCY–DATA PROTECTION INTERFACE

Many of the milestone cases that will be discussed below were also a step that signaled an end to the era of the happy co-existence of the insolvency and data protection laws. In other words, the period when data protection did not interfere in the administration of insolvency proceed-

56 Note that although regulations "are part of national legal systems, without the need for transformation or adoption by national legal measures ... Member States may nonetheless need to modify their law in order to comply with a regulation, or they may need to pass consequential legal measures in order to give full effect to ... the regulation." (Craig, P., Búrca, G. de, 2020, p. 105). There is also no formal hierarchy between regulations, directives, and decisions, i.e., the mandatory sources of EU law. Thus, "[r]egulations are not 'superior' to directives." *Ibid.*, p. 143.

57 *Ibid.*, p. 145.

ings and did not cause major new problems came to an abrupt end at some point around the end of the first decade of the 21st century. This was due primarily to the technological advancements that drastically increased the exposure of personal data to new types of threats and the parallel expansion of data protection laws. For example, the abovementioned *Google Spain* case contained several elements familiar to bankruptcy lawyers, i.e., the forced sale of a once bankrupt debtor's assets and related internet postings, which had become obsolete but nonetheless remained online.

Part of the story is that practice had already proven that offline methods for informing creditors, other stakeholders, and the public at large about the opening, closure, and other important steps in insolvency proceedings did not work satisfactorily in the cross-border context.[58] While the European Insolvency Regulation (EIR) 2000 still had to grapple with classical offline methods of publicizing various data (e.g., "notices in newspapers and official government gazettes, the posting of notices on court bulletin boards, the sending of individual notices to known creditors"),[59] in the intervening period, notification through online insolvency registers has become the dominant notification method throughout Europe due to technological advancements. Insolvency lawyers have welcomed new technologies as tools for solving these problems. So much so that by the time work began on the 2015 Recast EIR, online publication was widely – though not ubiquitously – accepted[60] throughout Europe. This progressive transformation elicited reactions from both data protection and insolvency lawyers in Europe. As will be detailed in the following pages, the result is a new chapter in the recast EIR devoted to data protection and the myriad new questions demanding answers.[61] Thanks to these, the data

58 Veder, M., Article 24 – Establishment of insolvency registers, in: Bork, R., Zwieten, K. van, (eds.), 2022, *Commentary on the European Insolvency Regulation*, Oxford, OUP, p. 385.

59 *Ibid*.

60 According to a 2012 Report by the EU Commission, at that time, only 14 Member States published decisions made in insolvency proceedings online for access by the public, 9 other Member States had some information on insolvency available in electronic databases, and 4 Member States had no information on insolvency proceedings whatsoever available in electronic form. See Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No. 1346/2000 of 29 May 2000 on insolvency proceedings (COM[2012] 743 final), para 8, cited also in Veder, M., 2022, p. 387 n. 5.

61 As stated in the Proposal for a Regulation of the European Parliament and of the Council amending Council Regulation (EC) No. 1346/2000 on insolvency proceedings (COM(2012) 744 final), para 1.2: "There are problems relating to the rules on publicity of insolvency proceedings and the lodging of claims. There is currently no

protection–insolvency interface ought now be considered a distinct agenda item for both data protection and insolvency law.

3.5. DATA PROTECTION-RELATED NOVELTIES INTRODUCED BY THE 2015 RECAST EIR

The new provisions of the Recast EIR that attracted the most ire from data protection activists aimed to exploit new technologies to make the administration of cross-border insolvency cases more efficient by making it easier to access such data. The underlying policy presumption was and remains that "it is vital that publicity is given to the opening of insolvency proceedings, important steps to be taken during the proceedings, and the closure of the proceedings."[62] This is the interest of creditors, third-party debtors, banks, and the public at large, though for different reasons.[63]

Consequently, the Recast EIR required Member States to establish and maintain one or more electronic insolvency registers in their respective territories[64] and to make ten classes of insolvency-related information publicly available ("mandatory information") as soon as possible following the opening of such proceedings,[65] though the task of interpreting the scope of the "as soon as possible" standard was left to the courts. Unfortunately, there are still Member States in which there are no insolvency register through which insolvency-related information could easily be checked via the Internet; accessibility in other than the local language(s) is especially an issue. Moreover, the features of the insolvency registries also differ. For example, while in some of the Member States there are registers specifically dedicated to insolvency, in others insolvency-related data is in registers devoted also to other types of data and there are also differences in the nature of data and information made accessible.[66]

mandatory publication or registration of the decisions in the Member States where a proceeding is opened, nor in Member States where there is an establishment. There is also no European Insolvency Register which would permit searches in several national registers. However, the good functioning of cross-border insolvency proceedings relies to a significant extent on the publicity of the relevant decisions relating to an insolvency procedure. Judges need to be aware whether proceedings have already been opened in another Member State; creditors or potential creditors need to be aware that proceedings have commenced" (according to Veder, M., 2022, p. 387).

62 *Ibid.,* para 24.01, p. 385.

63 *Ibid.*

64 Recast EIR, Art. 24(1).

65 *Ibid.*, second sentence.

66 See the European e-Justice Portal, page with general information on insolvency law and insolvency registers of the Member States (https://e-justice.europa.eu/110/EN/bankruptcy_and_insolvency_registers, 7. 9. 2023).

In addition to mandatory publicizable information, two other express provisions enhance access to data, and thus may affect data protection lawyers. One allows Member States to require the recording of additional personal data by or the filing of documents containing such data with their national insolvency register. A good example is the insolvency-related disqualification of directors.[67]

The other gives Member States the freedom to either include information on individuals not exercising any independent business or professional activity into the insolvency registers, or to make such information publicly available through a system of interconnected insolvency registers.[68] The latter choice was added in order to "[tackle] the disparities that [existed and continue to exist] in the laws of the Member States on the extent to which the overindebtedness of consumers is dealt with in insolvency law and seeks to protect the privacy of such individuals."[69] As a counter-balancing measure aimed to protect foreign creditors, it is also prescribed that in cases where no such individual-related information is included in insolvency registers, known foreign creditors are to be informed about the opening of insolvency proceedings immediately, either by the court having jurisdiction or by the insolvency practitioner they appoint.[70] Although no sanctions are foreseen for non-compliance, foreign creditors not informed on the opening of insolvency proceedings cannot suffer negative consequences thereby.[71] Obviously, it remains to be seen whether these provisions can work efficiently in practice.

The more important novelty, however, is that a new decentralized system connects the aforementioned national insolvency registers through a so-called e-Justice Portal, "a central public electronic access point to information in the system."[72] This system, established by the EU Commission,[73] provides a search service in all official languages of the institutions

67 Recast EIR, Art. 24(3).

68 *Ibid.*, Art. 24(4).

69 Veder, M., 2022, p. 388, n. 60.

70 Recast EIR, Art. 54(1).

71 *Ibid.*, Art. 24(4), second sentence.

72 *Ibid.*, Art. 25(1).

73 The EIR contains detailed rules on the role of the EU Commission, basically the [executive] government of the EU, that is to play a central role in the maintenance of the new system. To wit, the Recast EIR's new Chapter VI on data protection establishes the decentralized system (Art. 25(1)) and regulating its technical aspects (Art. 25(2)), as well as empowering the Commission as the *controller* for processing personal data (Art. 80(1) Recast EIR). Put simply, the EU Commission plays the key role with respect to the new e-Justice Portal's insolvency prong, including defining the necessary policies (Art. 80(2)), implementing the various technical measures necessary for fulfilling its responsibilities as controller (Art. 80(2)), and ensuring the confidentiality

of the Union, thereby making both mandatory and any optional information from national insolvency registers available to the public, alongside other publicly accessible documents.[74] To make the new system more user-friendly, the Recast EIR requires the envisaged search facilities and services to be free of charge,[75] and the system is to operate fully electronically in order to ensure easy access from any point of Europe (and beyond) through a single "central electronic access point."[76]

3.6. "TECHNOLOGIZED" CROSS-BORDER INSOLVENCY LAW AND THE CONCOMITANT INCREASED DATA PROTECTION RISKS

As one may expect, the abovementioned and other such technological advancements that enhance ease-of-access to sensitive personal data are also factors that increase risk and raise unresolved questions corollary to the data protection–insolvency law interface, as will be demonstrated by some of the milestone cases discussed below. For data protection scholars, policy-makers, and human rights activists, the envisaged pan-European electronic system was not seen merely as an efficiency-enhancing tool for cross-border insolvency proceedings, but also as a measure that would drastically increase the risk of personal data being exposed. As the European Data Protection Supervisor (EDPS) put it in its 2013 Opinion on the Commission proposal for a Regulation amending Council Regulation (EC) No. 1346/2000 on insolvency proceedings, European data protection legislation must be applied here because "[a]mongst the measures proposed that will impact data protection, the [new insolvency regulation] Proposal provides for a mandatory publication of the decisions opening or closing a proceeding and encourages and organises cross-boarder [*sic*] exchanges of information between stakeholders. ... Information thus published and/or exchanged may identify (either directly or indirectly) debtors, creditors, and liquidators involved in the proceeding."

Furthermore, the EDPS found that there are "shortcomings and inconsistencies in the way the proposed [insolvency] Regulation [i.e., the then prospective Recast EIR 2015] deals with issues related to/concerning

---

and integrity of any transmission from the European e-Justice Portal (Art. 80(3)). Analogous responsibilities concerning the processing of personal data in the insolvency registers themselves are allocated to the Member States (Art. 79).

74 Recast EIR, Art. 25(1), second sentence.

75 *Ibid.*, Art. 27(2). The Member States may, however, charge a reasonable fee for access to the documents or additional information even if via the system of interconnected insolvency registers as per Recast EIR Art. 27(2).

76 Veder, M., 2022, p. 391, n. 60.

personal data."[77] These concerns, and related consultations involving the two sides (i.e., protagonists of insolvency transparency versus data protection positions), eventually led to the addition of Chapter VI on data protection to the Recast EIR. The new Chapter VI – a rather short one[78] – divides competences and responsibilities for the implementation of the chapter among Member State bodies and the European Commission, and invokes the generally applicable data protection legislation. Thus, despite the importance of the data protection–insolvency law interface to insolvency practitioners, Chapter VI's text provides neither them nor others unfamiliar with the ins-and-outs of EU data protection law with much in the way of guidance on the said interface.

3.7. THE REMOTE RISKS: THE IMPACT OF DECISIONS BASED ON EUROPEAN CONSTITUTIONAL AND HUMAN RIGHTS LAW

There is a remote – yet real – possibility that future decisions based on European constitutional[79] and human rights law may also affect insolvency law. The fact that Europe has evolved a branch of data protection law distinct from privacy law does not mean that the interaction between data protection law and constitutional/human rights law will cease. As a consequence, future developments in these overlapping domains may also affect insolvency lawyers.

This deserves greater attention because of the fact that Europe possesses two partially overlapping and partially competing "constitutional" and/or "human rights" systems, each with a highly influential court at its pinnacle. These are, of course, the European Court of Justice, the supreme court of the European Union, seated in Luxembourg, and the European Court of Human Rights, headquartered in Strasbourg, France. Although their missions differ, today either court could rule on cases concerning data protection issues that might also impact insolvency law. New issues and new solutions thereto should also be expected, especially due to the

77 Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation amending Council Regulation (EC) No. 1346/2000 on insolvency proceedings, *OJ* C 358, Section 1.3.(9), 7 December 2013, pp. 15–16.

78 Recast EIR Chapter VI, devoted to data protection in the context of cross-border insolvencies, has altogether six articles (Arts. 78–83).

79 For a review of protection of human rights in the EU see Beširević, V., The Constitution in the European Union: The State of Affairs, in: Dupeyrix, A., Raulet, G. (eds.), 2014, *European Constitutionalism. Historical and Contemporary Perspectives*, Brussels, Peter Lang, coll. Euroclio, pp. 15–35.

unprecedented dynamics and prestige that data protection has acquired in Europe over the past several decades.

Any discussion on the genesis of, characteristics of, and relationships between the Luxembourg and Strasbourg courts and the associated systems is unfortunately inherently complex, because their relationship is presently in a state of limbo. A rough outline is hopefully nonetheless sufficient for the purposes of casting light on why this relationship matters for insolvency lawyers. At present the judgments, neither of the Luxembourg, nor of the Strasbourg Courts give any particular cause for concern, but the unresolved relationship between the two does bring the topic into the limelight. Let us take a closer look at these, to better assess what is at stake.

3.7.1. The Stance of the European Court of Justice: Exclusive Autonomy in Lieu of a Discursive One

Let us start by quoting Craig and de Búrca, the authors of the top textbook on EU law, according to whom "[p]rior to the enactment of the Charter of Fundamental Rights [in 2009], the main international instrument for the protection of human rights drawn upon by the ECJ as a *'special source of inspiration'* was the European Convention on Human Rights."[80] After ECJ Opinion 2/13, however, this seemingly happy co-existence has morphed into the opposite, with the practical effect being that there is now basically no certainty whatsoever regarding whether, when, and in what form the Luxembourg court would draw on the decisions of the Strasbourg Court. The main milestones of the road that led to this state of affairs are as follows.

The predecessor of today's European Union, the European Economic Community, was formed in 1957 and focused on economic cooperation. Human rights were not part of its initial framework, despite the fact that one of the key motivations behind the Community's creation was the desire to prevent a third World War by enhancing cooperation between France and Germany. Indirectly, therefore, it was done in response to the horrors and human rights violations of WWII. It was gradually realized, however, that "ever closer economic cooperation could equally affect human rights standards."[81] Thus, in this first phase, human rights-related considerations appeared only in some of the judgments of the Court.

80 Craig, P., Búrca, G. de, 2020, p. 435, (emphasis by author).

81 Kuijer, M., 2020, The Challenging Relationship between the European Convention on Human Rights and the EU Legal Order: Consequences of a Delayed Accession, *The International Journal of Human Rights*, Vol. 24, Issue 7, pp. 998–1010, p. 1000.

This stance changed with the 1992 Maastricht Treaty, which contained nothing less than a declaration enshrining European law's human rights dimension,[82] but there was at that point no clear path forward with regards to how this declaration should to be implemented. Some suggested that the EU should have its own instrument of human rights, and others that the EU ought to accede to the ECHR. Rather than choosing one option, both were pursued simultaneously, and thus the route proceeded along two separate and meandering paths.

The next milestone was the Constitution for Europe (TCE), which foresaw the possibility of the EU acceding to the ECHR,[83] but this proposed Constitution was rejected in France and the Netherlands. Probably out of political caution in the aftermath, the Lisbon Treaty was not enacted until 2009.[84]

The Lisbon Treaty led to the adaptation of the EU Charter of Fundamental Rights,[85] an instrument similar to – and to a significant extent overlapping with – the Council of Europe's ECHR.

As far as the question of accession to the ECHR was concerned, the Treaty stipulated that the EU Commission would ask the ECJ to give an opinion on the EU's competence to conclude an agreement on accession.[86] ECJ Opinion 2/13, which prevented accession, "raised eyebrows" and provoked rather fierce critique; some critics went as far as to claim that the Opinion was intent on killing off accession, thereby making external oversight impossible. While opinions are considered a form of "soft law" in EU law (i.e., they lack binding force and direct effect),[87] they matter nonetheless, as Opinion 2/13 amply demonstrated that in practice; as just described.

3.7.2. The Possible Impact of the Decisions of the European Court of Human Rights

Today, while the privacy and data protection-related decisions of the European Court of Human Rights (ECtHR) certainly have the potential to impact insolvency law, the nature of this impact is too uncertain for it to be worth the attention of insolvency practitioners, at least for the

82 *Ibid.,* p. 1000.

83 Article I-7 §2 states: "The Union shall seek accession to the European Convention for the Protection of Human Rights and Fundamental Freedoms."

84 *OJ* C 306, 17 July 2009. Entry into force on 1 December 2009.

85 Charter of the Fundamental Rights of the European Union, *OJ* C 83, Vol. 53, EU, 2010, p. 380.

86 Based on Article 218(11) TFEU.

87 Craig, P., Búrca, G. de, 2020, p. 146.

time being. This, however, does not mean that this potential impact is unlikely to occur. *A fortiori*, the more intense the interplay of bankruptcy and data protection law becomes, the higher the chances that decisions by both the Luxembourg and Strasbourg courts will impact insolvency proceedings across Europe, as well as extra-judicial workouts (i.e., out-of-court restructuring agreements between the creditors and the insolvent, or near-insolvent debtor) and preventive restructuring equivalents. For one, the Council of Europe system, the pan-European protector of human rights, has its own instrument in the domain: the 1981 Convention for the Protection of Individuals with Regard to the Processing of Personal Data, also known also as Convention 108. Strasbourg has always attempted to keep pace with the drastically increasing importance of data protection, primarily under the influence of EU developments in the area,[88] but also as a result of the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), promulgated in 2018[89] and resulting in a "modernized" Convention.[90] Mention could also be made of the Council of Europe Convention on Access to Official Documents (CETS No. 205), referred to also as Tromsø Convention.[91]

These factors suggest that a day will come in the not-too-distant future when the Strasbourg court will make a decision affecting bankruptcy

88 As the Explanatory Report for Convention 108+ expressed: "With regard to the EU data protection reform package in particular, the works ran in parallel and utmost care was taken to ensure consistency between both legal frameworks. *The EU data protection framework gives substance and amplifies the principles of Convention 108* and takes into account accession to Convention 108, notably with regard to international transfer," (emphasis by author). See Council of Europe, 2018, Convention 108+: Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Explanatory Report para. 4, p. 15 (https://edoc.coe.int/en/international-law/7729-convention-108-convention-for-the-protection-of-individuals-with-regard-to-the-processing-of-personal-data.html#, 21. 10. 2023). See also Zeitzmann, S., 2021, The Council of Europe's Tromsø Convention on Access to Official Documents, *European Data Protection Law Review*, 7, p. 232.

89 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018) 2-final, (https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168089ff4e, 7. 9. 2023).

90 CM/Inf(2018)15–final, consolidated text of the modernized Convention 108+ (https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf, 7. 9. 2023). As of August 2022, 55 states were parties to the Convention, (https://www.coe.int/en/web/data-protection/convention108-and-protocol, 7. 9. 2023).

91 Council of Europe, 2020, Council of Europe Convention on Access to Official Documents (CETS No. 205). See Ukrow, J., 2018, Practitioner's Corner – Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108, *European Data Protection Law Review*, Vol. 4, Issue 2, pp. 239–247, cited in Zeitzmann, S., 2021, p. 232, n. 5.

law for data privacy reasons, on the basis of the 1950 ECHR. Let us add to this that the ECtHR has already made decisions touching upon bankruptcy-related matters.[92] The effect of those decisions on insolvency practitioners in Europe depends, however, on whether the cooperative atmosphere between the two courts, which existed prior to 2009, will ever be restored. Understanding the history of this falling-out is of utmost relevance for insolvency lawyers, and so requires a brief canvassing of the constitutional dimensions of the link that has existed and continues to exist today.

Namely, the EU's 2009 Lisbon Treaty[93] took the fundamental step toward making the EU Charter legally binding, and with a status co-equal with the Treaties themselves. This acted as a catalyst that brought to the surface the fundamental constitutional issues concerning the relationship between the Luxembourg and Strasbourg courts.[94] One of the consequences of the consolidation of fundamental rights in the treaty was the exacerbation of the trend that pre-dated the 2009 Opinion 2/13; the CJEU's demonstrably stronger and more frequent reliance on the EU's own Charter of Fundamental Rights,[95] a shift that could not but be paralleled with a subtle decrease in the ECtHR's influence.

Yet the textual basis for a divergence of Europe's two supranational human rights systems, which itself increased the chances of potentially differing interpretations, radically changed shortly afterwards, through CJEU Opinion 2/13,[96] which proclaimed that the Draft Agreement on the Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms was not com-

92 See, in particular, the Moldovan cases of *Banca VIAS* 32760/04 (judgment delivered on 6 November 2007) and *Oferta Plus SRL* (14385/04 judgment delivered on 12 February 2008). For facts and a concise elaboration of the cases see Svetlicinii, A., Enforcement of Contracts in the Republic of Moldova: The Impact of a Slow Transition, in: Messmann, S., Tajti, T. (eds.), 2009, *The Case Law of Central and Eastern Europe – Enforcement of Contracts*, Vol. 1, Bochum, European University Press, para 1.6., pp. 449–456.

93 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community (*OJ* C 306, 17 December 2007). It entered into force on 1 December 2009.

94 Kuijer, M., 2020, p. 1001.

95 See Kuijer, M., 2020, pp. 1001–1002, citing Búrca. As per Kuijer, according to the relevant research conducted, the CJEU referred to ECHR 7,5 times more than to all other human rights instruments (including the Charter), during the period from 1998 to 2005 (when the EU Charter was not binding), but that has radically changed since 2009: the CJEU has referred to the Charter in 122 cases but has only invoked the ECHR on 20 occasions. See Búrca, G. de, 2013, After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator? *Maastricht Journal of European and Comparative Law*, 20, p. 168.

96 Opinion 2/13, EU:C:2014:2454 (18 December 2014).

patible with EU law for a number of reasons. In particular, the CJEU has exclusive jurisdiction to decide all issues of EU law, while the Agreement by contrast allows the ECtHR to decide on EU law matters.[97] The 43-page Opinion raised numerous complex constitutional issues and was criticized rather than praised by the vast majority of scholars in the field,[98] and was viewed with "a combination of shock, disbelief and protest,"[99] and as "a legal bombshell".[100]

The practical effects of the Opinion, the significance of which can be grasped even by those unfamiliar with EU constitutional law,[101] however, are not just of importance for the future of the bankruptcy-data protection interface and to this article: the Opinion simply prevented the EU's accession to the Convention. Practically, this means that until negotiations result in a formula capable of changing this state of affairs, the CJEU will remain the exclusive interpreter of EU constitutional and human rights law, and therefore also of the EU's privacy and data protection law. Still, it would be a mistake to completely exclude the possibility that the ECtHR's past or future decisions will continue to serve as a source of inspiration, though admittedly – and to stress again – this seems to be a very remote risk for insolvency lawyers at present.

In other words, as there is already a *real* and *an already existent risk* that national data protection authorities will knock on the doors of insolvency practitioners in concrete insolvency proceedings (as illustrated by the Hungarian case below), the chances of the appearance of CJEU decisions directly affecting insolvency law could be assessed as *remote*, and the possibilities of the surfacing of ones of the Strasbourg Court – the *remotest*. Nonetheless, whether these risks are academic matters that should not worry insolvency practitioners and others coping with the myriad challenges corollary to bankruptcy law, should perhaps be assessed in a year or two.

97 Kuijer, M., 2020, p. 112.

98 For an elaborate analysis, supporting some aspects of CJEU's reasoning, see Halberstam, D., 2015, It's the Autonomy, Stupid! A Modest Defense of Opinion 2/13 on EU Accession to the ECHR, and the Way Forward, *German Law Journal*, Vol. 16, Issue 1, p. 105.

99 Scheinin, M., 2014, CJEU Opinion 2/13 – Three Mitigating Circumstances, *VerfBlog,* December 26, (http://www.verfassungsblog.de/cjeu-opinion-213-three-mitigating-circumstances, 7. 9. 2023).

100 Buyse, A., 2014, CJEU Rules: Draft Agreement on EU Accession to ECHR Incompatible with EU Law, *ECHR Blog*, December 20, cited in Kuijer, M., 2020, n. 29 (blog text no longer available online, as of 15 August 2022).

101 From a US perspective, the opinions of the CJEU are a peculiar source of law because the CJEU – essentially the Supreme Court of the EU – is empowered to pass them even if there is no "case or controversy", a prerequisite for Supreme Court jurisdiction in the US. See also Kuijer, M., 2020, pp. 1004 ff.

3.8. THE INSOLVENCY–DATA PROTECTION INTERFACE IN THE UNITED KINGDOM AFTER BREXIT

Since the expiry of the Brexit[102] transitory period (i.e., withdrawal of the UK from the European Union) on 1 January 2020, the Data Protection Act 2018[103] has been the UK's governing data privacy law, though the UK government's website states: "[t]he Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR)."[104] Even the UK's best industrial publications make plain that UK data protection law rests on identical foundations as that of the EU, and these foundations have remained of crucial importance in the Isles, in particular to reducing complex and expensive compliance burdens on companies with affiliates on the Continent or who are doing business there. As emphasized by the European Data Protect Office (EDPO), in most circumstances, not one but two Data Protection Representatives need to be appointed in cross-border cases implicating business in both the EU and the UK, due to the requirement to comply with both the EU GDPR and the new UK equivalent.[105]

4. What European Case Law Can Tell Us About the Interface: European Court and Data Protection Authority Decisions

The extreme dynamics of European data protection law outlined above will likely intensify rather than subside in the near future, and this cannot but create novel privacy concerns for bankruptcy, similarly to what has been the case in both Canada and the US. The slowly emerging jurisprudence – be it in the form of decisions by various national Data Protection Authorities (DPAs) or by courts adjudicating unforeseen legal issues in the bankruptcy–data protection interface shows that in Europe, just like Geist noted with regards to Canada, "there is [often] no satisfactory answer to be found in the current law."[106] The following examples are intended to illustrate the sorts of difficulties Europeans

102 For a review of Brexit see, e.g., Beširević, V., A Short History of Brexit, in: Ilić, T., Božić, M. (eds.), 2020, *NOMOPHYLAX: Collection of Papers in Honor of Srđan Šarkić*, Belgrade, PFUUB – Službeni glasnik, pp. 621–645.

103 The Data Protection Act, UK Public General Acts 2018 c. 12.

104 See https://www.gov.uk/data-protection, 7. 9. 2023.

105 EDPO, Brexit and the Data Protection Representative – What Is the Impact for Your Company?, (https://edpo.com/uk-representative, 7. 9. 2023).

106 Geist, M., 2002, p. 70.

have faced and presumably will continue to face, probably with greater frequency, in the future.

As a preliminary caveat, it should be noted that unlike Canada and the US, which were exposed to the challenges attendant to the bankruptcy–data privacy interface over the same period as the Europeans (in some respects even earlier), fewer relevant cases are reported on the Old Continent and thus the amount of case law material available for researchers is less, especially if only English-language material is considered. This is so not only because of the language barrier and the dominant civil law tradition's tendency to report a comparatively modest percentage of total court and agency cases, but because in Europe bankruptcy stigma remains fairly strong, even in countries like Germany – the economic engine of Europe. As a result, there is less willingness in Europe to participate in various bankruptcy-related processes, and the number of companies abandoned rather than liquidated – let alone reorganized – is staggeringly high,[107] especially in some post-socialist (communist) states in Central and Eastern Europe (CEE), including *inter alia* the west-Balkan countries of Serbia, Montenegro, and Bosnia and Hercegovina.[108]

A behavioral factor inevitably also impacts research in the data protection domain. In the author's experience, many national DPAs are not keen to respond to queries from interested scholars. Moreover, their stance may change over time, due to staff changes or even political factors. These technical hardships require mention because it is difficult to even come close to getting an accurate picture of Europe's data protection–bankruptcy law interface when it is the aggregate confluence of such diverse and often intangible or unmeasurable factors.

The identified cases involving the bankruptcy-data protection interface can tentatively be divided into three major groups, each illustrated by one or two cases below. The first group includes straightforward cases where data protection law is simply applied in the bankruptcy context, as illustrated by the Hungarian DPA[109] case in the next sub-section. Here there is no need for balancing, though courts or authorities obviously have discretionary and interpretative powers available to them when necessary. By contrast, in the second group of cases, the decisions

107 See, e.g., Tajti (Thaythy), T., 2019. Unprotected Consumers in the Digital Age: The Consumer-creditors of Bankrupt, Abandoned, Defunct and of Zombie Companies, *Tilburg Law Review*, Vol. 24, Issue 1, p. 3.

108 For further insight see, e.g., Tajti (Thaythy), T., 2017, Leasing in the Western Balkans and the Fall of the Austrian Hypo-Alpe-Adria Bank, *Pravni Zapisi*, Vol. VII, No. 2, pp. 155–221.

109 Case NAIH-2087–5/2012/H (March 2012) (in Hungarian language).

were made by balancing and prioritizing the policies and rules of bankruptcy and data protection laws. The German case concerning the unpaid honorariums of a psychotherapist exemplifies this group of cases.

The third and most complex group of cases (at least in the author's opinion) showcase the different modalities and effects of *conflicts* between insolvency and data protection law. While in the Italian case below, data protection law frustrated the sale of genetic data collected in the Sardinian Ogliastra region during insolvency proceedings, the UK pre-Brexit insolvency case of *Re Southern Pacific Personal Loans Ltd.*[110] goes further still because it demonstrates that at least two systemic antagonisms exist between these two branches of law. The details follow.

4.1. THE "HEALTHY CO-EXISTENCE" GROUP OF CASES

Although it is presumably not the only such case in Europe, the Hungarian DPA's decision to impose fines on a liquidator is nonetheless paradigmatic of the implementation of data protection law in the domain of bankruptcy law – something that may happen to any bankruptcy practitioner that fails to either educate him– or herself in (or to correctly apply data protection regulations when) handling bankruptcy cases. In the case, a penalty amounting to five million forints (HUF) (EUR 16,000 at the time) was imposed because the liquidator kept insolvency case files in an unguarded doorless stable, and these were therefore accessible by the public. Data protection regulations applied as the documents in question contained sensitive personal information, and the applicable data protection regulations protected medical reports, personal identification documents, along with driving licenses, as well as employment-related documents and social security cards.

The lesson to be learned from this case is simple: insolvency practitioners must educate themselves in data protection law, keep track of pertinent changes, and comply with the law in their practice; the alternative is facing increasingly high penalties. In cases involving big-ticket international corporations, especially under the new GDPR, the penalties imposable have become enormous.[111]

The story unfortunately does not end here because insolvency practitioners may also be held liable as tortfeasors for the harm and damages

110 *Re Southern Pacific Personal Loans Ltd.,* [2013] EWHC 2485 (Ch).

111 As per GDPR Article 83(5), the imposable penalty can go up to €20m or 4% of an undertaking's total global turnover of the preceding fiscal year. GDPR Art. 58 (Powers), Art. 70 (Tasks of the European Data Protection Board), Art. 83 (General conditions for imposing administrative fines), and Art. 84 (Penalties) are also of relevance.

caused by infringing data protection laws in some cases, in addition to being fined. This possibility has already been discussed by some courts.[112]

4.2. CASES PREMISED ON BALANCING AND PRIORITIZING

In this section, the 2009 German Supreme Court (*Bundesgerichtshof*) judgment[113] is given short shrift in order to get to the main point without further ado. The factual background was simple: insolvency proceedings were opened against a psychotherapist who had outstanding claims for his clients' unpaid fees. When the bankruptcy practitioner (trustee) asked the debtor to transfer the documents containing his client-obligors' personal data, he refused to do so, invoked the doctor-patient confidentiality rule, and was generally uncooperative. To break this impasse, the court had to balance applicable policies. Eventually it ruled that "the need for revealing data on patients to the insolvency practitioner enjoys priority over the claim of the patients for protection of their data ... Should the contrary position of the debtor applied, the conduct of insolvency proceedings would not be possible in case the debtor is a medical doctor working exclusively with private patients."[114]

In the 2016 case, decided by the District Court of Rockenhausen (Germany),[115] however, the balance tilted in favor of data protection law. At stake was a cell-phone insolvency application that gave users access to the insolvency-related data of more than a million German companies and individuals, accounting for roughly 98% of all the debtors in Germany.[116] Individual data could be located not only by searching the names of debtors, but also by searching for their places of residence, in case of several individuals place of residence shown also on a map of Germany. What made the case peculiar is that the data was based on publicly accessible entries from insolvency registers. Yet – at least according to the opinion of the court – due to the simplified search possibilities, the otherwise public data acquired a different quality, and therefore the app infringed data protection laws, especially due to its "shaming effects" (*Prangerwirkung*) on debtors.[117]

112 See, e.g., *London Oil and Gas Ltd (In Administration*), [2019] EWHC 3675 discussed below. According to the court, as they are agents of the company in administration, they are also potential tortfeasors. *Ibid.,* para. 2.

113 BGH IX ZB 85/08 (5 February 2009).

114 *Ibid.,* point 5. Translation by the author.

115 *AG Rockenhausen*, Urt. V. 09 August 2016 Az 2C 341/16.

116 *Ibid*., description of facts.

117 *Ibid.*

4.3. CONFLICT CASES

4.3.1. Frustration of Bankruptcy Goals: The Italian *Shardna* Case

Another case with an unexpected turn, which precluded the realization of one of insolvency law's key goals – i.e., the sale of the debtor company's valuable assets – concerned the insolvency of an Italian limited liability company named Shardna, whose most valuable asset was genetic data collected in the Sardinian Ogliastra region, which is famous for being home to an extraordinary number of centenarians.[118] After a change in Shardna's top governance structure, it became the subject of a controversial insolvency proceeding, whereby it was sold to a UK biotechnology company's Italian subsidiary (Tiziana Life Sciences). This purchase was motivated by the possibility of commercially exploiting the estate, which most importantly possessed "the right to use the biological samples, the declaration of consent by participants, the equipment and the content of the biobank as well as the database comprising the medical histories of the donors."[119]

The plans of the acquiror, however, could not be realized due to a specific legal regime preventing the disposal of this class of assets.[120] Moreover, the EU Commission subsequently confirmed, in response to a related question raised in the European Parliament, that biological samples are "able to reveal information which [refer] to an identified or identifiable person," and as a result are protected as personal data.[121]

4.3.2. *Re Southern Pacific Personal Loans Ltd:* Data Protection Law as Red-Tape

All regulations create red tape. Today, in the age of the regulatory state, this should be common knowledge. Data protection law is no exception. The forms in which red-tape appears and its onerousness range from simple to complex, and while some forms of data protection red tape are relatively easy to deal with, others generate complex systemic issues.

Moving forward, bankruptcy courts should be prepared to pay special regard to personal data, as well as ensure they are in a position to provide guidance for various insolvency practitioners (and others who potentially have access to personal data in various documents or electronic databases)

118 The synopsis of the case is based on Piciocchi, C. *et al.*, 2018, p. 181.

119 *Ibid*., p. 182. Cited also in Bork, R., Zwieten, K. van, 2022, para. 78.13.

120 The conditions that applied to them were regulated by Italian Legislative Decree 196/2003. See Piciocchi, C. *et al.* 2018, p. 182.

121 Piciocchi, C. *et al.* 2018, p. 182.

in order to guarantee the proper implementation of data protection laws. No simple, generally-applicable formula seems to exist because the cases involving this interface are so fact-sensitive. Moreover, personal data protected by European data protection laws may be in documents or electronic databases (e.g. email exchanges) alongside confidential and/or privileged information normally not protected by data protection but by other laws, as it was in the 2019 UK case *London Oil and Gas Ltd (In Administration)*.[122] Numerous related dilemmas can emerge – as the case demonstrates – such as how to conceive a method to determine to which documents insolvency practitioners should have access to and which they should not, who should bear the costs of such a search, and what is the best method of ensuring that related processes do not unnecessarily disrupt the administration of bankruptcy cases. The hinted-at selection is a task that can be performed if the court is capable of formulating appropriate search-terms to limit the number of accessible documents.[123]

What *Southern Pacific* (a case that unearthed two systemic problems) showed was of crucial relevance to the bankruptcy–data privacy interface and was related to two essential questions that both fundamentally affect the "bankruptcy mathematics" (namely, the expected returns of creditors calculated based on average recoveries) and the underlying core principles. The first is that it showed how prohibitively expensive the implementation of the European data protection system could be in the specific context of insolvency proceedings. The second consequence was the realization that the enforcement of data protection regulations directly affects the rights of creditors and equity holders in insolvency proceedings, and the administration of bankruptcy cases more broadly. In short, data protection red tape has the potential to "eat up" a substantial part of the estate from which creditors and the costs of insolvency proceedings should be financed. This must have been a rude awakening for insolvency practitioners and others in the industry, both in the UK and elsewhere. The reactions seem to have remained conspicuously modest in Europe, though foreign creditors doing business with European partners, or having affiliates in the Old Continent, should heed to the lessons of *Southern Pacific* and hone their insolvency tactics accordingly.

The concrete and self-explanatory facts and quantitative data that the liquidators were faced with in the case, in brief terms, were the following. The debtor company provided personal loans to individuals in the UK, secured by way of a second mortgage on their homes, before it became insolvent. Although these were transferred to various Special Purpose

122 *London Oil and Gas Ltd (In Administration),* [2019] EWHC 3675, 2019 WL 08112165.
123 *Ibid.*

Vehicles (SPVs) in securitization projects, the title on the mortgages and the data remained with the debtor. Because of this, even after the debtor company went into voluntary liquidation, former clients aimed their requests for provision of related data (Data Subject Access Requests – DSARs) at the appointed joint liquidators. These requests, moreover, were typically blanket requests for a complete set of statements.[124]

The numbers were as follows. The cost of satisfying a DSAR was £455 exclusive of Value Added Tax (VAT) plus the fees payable to an outside loan servicing company (Acenden) for storing the data and providing related services.[125] According to the calculations of the joint liquidators, as 88 DSARs were filed per month, which cost £40,000 in total monthly, the yearly cost of satisfying DSARs could have foreseeably amounted to £589,000. As this amount had to be deducted from the estate, the continued implementation of data protection laws would have further reduced payments to creditors because according to estimations, only about £3m was available for distribution while liabilities totaled £10,297,000.[126] Per data protection law, the joint liquidators were deemed to be "data controllers" responsible for the proper implementation of relevant regulations and the provision of data to those who submit DSARs within 14 days.[127] Cognizant of the absurdity of the situation, the joint liquidators applied to the court, requesting clarification on the following question: may they refuse to comply with the DSARs, or alternatively, may they dispose of the data under their control?[128]

Although the court eventually allowed the joint liquidators to dispose of the data,[129] this was done based on a line of reasoning with which the Information Commissioner disagreed.

There is one last point that should be noted. Namely, the exorbitant red tape surfacing amidst liquidation proceedings in DSAR form concerned redeemed loans, documents, and data, "[n]one of [which was] any longer required for any business of the company or for any purposes of the liquidation, such as the realisation of assets."[130] This was the crucial factor that caused the court to direct the liquidators to dispose of this data in accordance with UK data protection law,[131] a move they justified by

124 *Southern Pacific,* para. 9.
125 *Ibid.*, para. 7.
126 *Ibid.*, para. 10.
127 *Ibid.*, para. 14.
128 *Ibid.*, p. 427.
129 *Ibid.*, para. 41.
130 *Ibid.*, para. 39.
131 *Ibid.*, para. 41.

invoking one of data protection law's basic principles, according to which "personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was processed."[132] Before this case, however, it had not been unequivocally clear whether liquidators and other insolvency practitioners had a right to do so. Moreover, *who* determines which data remains necessary and *when* it ceases to be necessary remains contestable.

Let us now take a look at the other problematic aspect of the case that concern the status of the joint liquidators under data protection law.

4.3.3. *Re Southern Pacific Personal Loans Ltd:* Can the Insolvent Debtor Company Be the Data Controller in Insolvency Proceedings?

The status – and therefore the powers, rights, and liabilities – of liquidators under data protection law was yet another fundamental but contested issue in the case. The way this issue was resolved affects not only the disposability of data, but also the potential administrative and criminal liability of liquidators.

The fact that there was a "tension" between the decision and reasoning of the court and the policies of data protection laws can be concluded already from the fact that while the Commissioner considered both the joint liquidators and the debtor company to be data controllers,[133] the court disagreed and held that they were not the controllers of data processed by the company prior to liquidation.[134] The consequence of this position was that the joint liquidators could not be held personally liable for non-compliance with data protection laws, such as – but not limited to – not responding to DSARs.[135] The essence of this case's long, somewhat artificial, yet complex reasoning, though supported by authoritative precedents, revolved around the question whether the liquidators were acting in the capacity of liquidators, or as agents of the debtor company. The court eventually opted for the latter. As was concluded in the related 2013 *Oakley Smith v. Information Officer* case,[136] "joint liquida-

132 *Ibid.*, para. 39.

133 *Ibid.*, para. 29.

134 *Ibid.*, para. 35.

135 *Ibid.*, para. 38.

136 *Oakley Smith v. Information Officer,* EWHC 2485 (Ch), 2013 WL 3994837 (2013). The case was initiated by the joint liquidators of Southern Pacific Personal Loans Limited. There was no respondent named and the "Information Commissioner (the Commissioner) was notified of the application and provided with the application notice and supporting evidence." *Ibid.*, para. 2.

tors are not data controllers for the purposes of the [Data Protection Act] as regards the data processed by or on behalf of the company in respect of the redeemed loans."[137]

Similar issues were adjudicated by the High Court in the post-GDPR case of *Dawson-Damer v. Taylor Wessing,*[138] which involved private trust litigation. The claimants were beneficiaries of a number of unfavorably restructured trusts, which eventually sued the trustees in the Bahamas and filed requests for access to personal data (DSARs). Three issues arose.[139] First, the solicitors (i.e., Taylor Wessing) objected with the argument that the claimants were exploiting data protection law as a discovery tool, as the so-acquired personal data was to be used in the Bahamian litigation. Contrary to old precedents, such as *Durant v. Financial Services Authority* 2003, where such data requests were rejected by courts on the basis that data protection law should not be used "as a proxy for third party discovery with a view to litigation,"[140] because access to personal data had been elevated to the level of a European fundamental right and further strengthened by the GDPR, the stance of UK courts had thus changed accordingly. Second, as in the aforementioned German case, Taylor Wessing here also unsuccessfully invoked the legal professional privilege (LPP) objection to justify its refusal to provide data.

The third issue was related to whether the request amounted to *disproportionate effort,* which as such could be rejected by Taylor Wessing, especially as old paper-form trust files were at stake. The court was of the opinion that the files were held in a "relevant filing system", and notwithstanding that some were organized in a chronological order and some not, the solicitors had to search these files for the claimants' personal data.[141] This detail is of relevance to us herein because the discovery–litigation–data protection interplay raises concerns similar to those raised by the data protection–insolvency law interface.

The 2019 *Green v. SCL Group*[142] case should also be mentioned, not only because it related to the 2018 Facebook–Cambridge Analytica

137 *Ibid.,* para. 51.

138 *Dawson-Damer v. Taylor Wessing* [2019] EWHC 1258 (Ch).

139 *Dawson-Damer v. Taylore Wessing LLP,* [2020] EWCA Civ 352, 2020 WL 01158643, para. 6.

140 Quoted and discussed in Brimsted, K., Evans, T., 2019, Data subject access requests – Three Illuminating UK Cases, *Privacy & D.P.,* Vol. 19, No. 7, p. 6.

141 Brimsted, K., Evans, T., 2019, p. 7.

142 *Green v. SCL Group Ltd* [2019] EWHC 954 (Ch); [2019] B.P.I.R. 833; [2019] 4 WLUK 301 (Ch D). Vincent John Green and Mark Newman were the joint Administrators of each of the companies involved in the Cambridge Analytica scandal, which acquired commercial data from multiple vendors, aggregated and analyzed the so-acquired

scandal,[143] but rather because the court agreed with the *Southern Pacific* case's holding that administrators are not data protection controllers.[144] Moreover, it further specified that consequently they are not required to respond to DSARs, nor is there any obligation on them to investigate data protection breaches by insolvent companies.[145] Instead, investigations are within the competence of the Information Commissioner's Office.[146] However, even here, the court admitted that "the implications of the Southern Pacific decision remain to be worked through;"[147] a comment that presumably refers to the ongoing and unresolved tensions inherent in the current state of the data protection–bankruptcy interface.

5. United States Perspectives

5.1. THE PRESENT STATE OF AFFAIRS: TOWARDS A COMPREHENSIVE DATA PRIVACY LAW?

As described briefly above, US data protection (or privacy law) is scattered across many pieces of legislation with no general statute akin to the European GDPR, leading to the very term "privacy law" often being apostrophized and compartmentalized into various sub-categories. This era of compartmentalized consumer data privacy law, however, has begun to gradually give way to a comprehensive one, a process that picked up pace post-COVID 19, primarily at the State-level, though in 2020 alone eleven comprehensive privacy bills were introduced in the Congress.[148] Following California, Virginia, Colorado, and Utah, Connecticut[149] was the fifth state to pass general data privacy regulations as of the time of writing.

---

data, and eventually used it for "micro-targeting", i.e., targeting individuals. Political parties and campaign groups also used their services to influence voting behavior. *Ibid.*, para 1. Part of the story was that the ICO raided the premises of Analytica, seized servers and substantial amounts of additional evidence, thereby making the work of Administrators impossible.

143 See Anonim., 2019 'Facebook to pay $5bn fine to settle Cambridge Analytica claim' – Case Comment, *Comp. & Risk*, Vol. 8, No. 4, pp. 1, 15.

144 *Green v. SCL Group Ltd*, para. 75.

145 Brimsted, K., Evans, T., 2019, p. 8.

146 *Ibid*.

147 *Green v SCL Group Ltd*, para. 72.

148 For the list see Chander, A., Kaminski, M. E., McGeveran, W., 2021, Catalyzing Privacy Law, *Minnesota Law Review*, 105, p. 1733, p. 1735, n. 7.

149 Substitute Senate Bill 6 (Public Act 22–15), signed into law on 10 May 2022, to step into force on 1 July 2023. See the blog of Rosenkotter, E., Wutscher, M., 2022, Fifth

The California statute – the California Consumer Privacy Act of 2018[150] (CCPA) – seems to have gone the farthest by introducing a "sweeping set of reforms" with "litany of protections" to consumers,[151] which is of major importance because much of the US technology industry is located in this state. In addition to the local kin of the European "right to be forgotten",[152] what is more important for our discussion is that according to this act consumers may prohibit sale of their data to third parties.[153] No wonder then that Schwartz attributed this to the impact of the GDPR.[154] Still, the Californian act – yet to be tested whether it has "teeth" or it is merely a "paper tiger" – represents a "sectoral model, narrower than the [European] GDPR,"[155] and it operates in a predominantly ex-post fashion, as opposed to the GDPR's ex-ante regulatory approach.

Irrespective of these recent vintage changes at the state level to some extent representing rapprochement with European data protection laws, the basic difference aptly canvassed by Schwartz and Solove in 2014 essentially still stands. As they put it, related to and through the central category of "personally identifiable information" (PII), "[t]he U.S. approach involves multiple and inconsistent definitions of PII that are often particularly narrow. The EU approach defines PII to encompass all information identifiable to a person, a definition that can be quite broad and vague."[156] Although the US legal category of PII is not equal to Europe's "personal data", they can be perceived as kins, the juxtaposition of which properly expresses the opposing fundamental philosophies on the two sides of the Atlantic that subsists to this day.

State in the Union Becomes Fifth State to Enact Data Private Legislation, *InsideARM,* 17 May, (9. 9. 2023).

150 California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798. 100–199 (West 2021) (came into force January 2020).

151 Akselrad, M. R., 2021, The Liquidation of Data Privacy: How and Outdated Bankruptcy Code Threatens Consumer Information, *Boston College Intellectual Property & Technology Forum*, 1, p. 8.

152 CCPA §§ 1798.100, 1798.105.

153 CCPA § 1798.120 ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.")

154 Schwartz, P. M., 2019, Global Data Privacy: The EU Way, *New York University Law Review*, 94, pp. 771, 810.

155 Nicola, F. G., Pollicino, O., 2020, The Balkanization of Data Privacy Regulation, *West Virginia Law Review*, Vol. 123, Issue 1, p. 63.

156 Schwartz, P. M., Solove, D. J., 2014, Reconciling Personal Information in the United States and European Union, *California Law Review*, 102, abstract p. 877.

5.2. THE KEY TOOLS FOR PROTECTING INDIVIDUALS' PRIVACY RIGHTS IN US BANKRUPTCY LAW

Heightened concern for privacy issues in US bankruptcy law was expressed quite early on, before such concern had been articulated in Europe or most other countries around the globe. First and foremost, concern about privacy issues is directly visible in very few provisions of the US Bankruptcy Code itself.[157] Section 363 is undoubtedly the most relevant here, which imposes restrictions on the use, sale, or lease of personally identifiable information on individuals. The issue is rather that these restrictions offer very limited protection to consumers, as illustrated by various cases, some of which are mentioned in this paper. Hence, it was properly noted by Akselrad that "[t]he heightened protections for customer privacy built into §363(b) of the Bankruptcy Code, aimed at remedying precisely these ills, seem poorly suited to handle the type of data in which social media and technology companies traffic today, putting almost nothing between those trying to acquire data and creditors who would benefit from its sale."[158]

Even though it is only remotely of any relevance, one should also not disregard Bankruptcy Rule 2004 on "examination" of an entity (including individuals, partnerships and corporations),[159] which essentially delineates the specific issues that may be examined by the court and which of them must remain protected as confidential matters. Specified circumstances that potentially impact bankruptcy proceedings may also be examined.[160] Although appearing as "confidentiality" and not as "privacy" matters, they should not be circumvented as their interplay may come up as an issue.

One should also mention less "visible" sources of law, such as the Policy on Privacy and Public Access to Electronic Case Files of the US Judicial Conference approved in March 2008, which initially protected

157 See in particular Bankruptcy Code sections 101(41A) and 363(b)(1).

158 Akselrad, M. R., 2021, p. 22.

159 Based on Bankruptcy Rule 2004, section (b), "entities" and the debtor may be examined with relation to the acts, conduct, property of the debtor, including liabilities and the debtor's financial condition. Entity, on the other hand, is defined under Section 101(15) of the Bankruptcy Code to include also "person", defined by Section 101(41) including – in addition to partnerships, corporations, and some governmental units – also individuals, which is the focus of our observations.

160 Rule 2004, section (b) of which reads that the examination of an entity or a debtor may relate "*only* to the acts, conduct, or property or to the liabilities and financial condition of the debtor" (emphasis by author), though also to "any matter which may affect the administration of the debtor's estate, or to the debtor's right to a discharge."

only debtors' social security numbers from public disclosure,[161] but later expanded this protection through amendments.[162] The EU GDPR lacks rules tailored specifically to insolvency, suggesting the conclusion that these are still awaiting the European courts and the drafters of bankruptcy laws of the Member States, given that substantive bankruptcy law remains national law.

The US's comparatively rich case law touching upon privacy matters in a bankruptcy context also merit mention. The practice shows, namely, that while the European data protection infrastructure has the advantage of being comprehensive, somewhat counter-intuitively, the US's narrower special legal regime for bankruptcy–data privacy offers more material for comparative scholarship.

5.3. THE 2005 AMENDMENTS OF THE BANKRUPTCY CODE: HEIGHTENED ATTENTION TO "PERSONALLY IDENTIFIABLE INFORMATION"

The central policy goal of the 2005 Bankruptcy Abuse Prevention and Consumer Protection Act[163] was to combat abuse of the bankruptcy system by individuals capable of paying their debts but nonetheless turning to bankruptcy courts to discharge them and "to keep a minimally necessary amount of [their] property."[164] What is less known is that this amendment to the Bankruptcy Code, which included the adoption of Chapter 15 for cross-border cases and the "means test" as a "trigger for a presumption of ... abuse"[165] by individual debtors, also made an important advancement in the protection of consumer privacy information, mainly in response to lessons learned from the 2000 *Toysmart.com* bankruptcy case.[166] This

161 Rhodes, S. W., 2003, Bankruptcy Decisions on Privacy Issues, prepared for American Bankruptcy Institute 2003 Annual Spring Meeting, April 10–13, ABI 557, paras. 7–8.

162 The text of the policy is available at https://www.uscourts.gov/rules-policies/judiciary-policies/privacy-policy-electronic-case-files, (1. 3. 2023).

163 Pub. L. No. 109–8, 119 Stat. 23 (2005).

164 Tabb, J. C., 2020, §1.1., p. 4.

165 *Ibid.*, §2.6, p. 149.

166 See *In re Toysmart.com Inc. LLC*, No. 00–13995 (Bankr. D. Mass., 17 August 2000), in which the court rejected the FTC – Toysmart settlement that placed several restrictions on the sale of the private consumer information in Toysmart's possession notwithstanding the existence of a policy in which the debtor (Toysmart) promised not to share such information with third parties ever, and the preceding *Federal Trade Commission v. Toysmart.com Inc.,* No. 00–11341-RGS, in which the settlement was announced and the complaint filed (D. Mass., 21 July 2000). See, Baxter, M. St. P., 2018, The Sale of Personally Identifiable Information in Bankruptcy, *American Bank-*

early regulatory reaction shows that the US began tackling the bankruptcy–data privacy nexus earlier than the Europeans – and presumably the rest of the globe.

As a reminder, the basic rule is that one of the responsibilities of the trustee (or of the Debtor-in-Possession in reorganization cases) is to sell or lease the estate's assets. Applying this basic rule in data protection cases means that the trustee is required to sell any data and information if there is a market demand for them. The task of the lawmaker was thus "to strike an efficient and just balance between the needs of the bankruptcy estate and the rights of all interested parties,"[167] with the latter including consumers and individuals whose personal privacy rights are at stake. The response of the US lawmaker was partial only: safeguards were introduced only with respect to liquidation (Chapter 7) proceedings, but not for Chapter 11 reorganizations. Because of this, some commentators see in the crucial section 1129 (which concerns confirmation of the reorganization plan) as "a dormant threat to consumer information" because "the immutable progression of technology aimed at cultivating user data necessitates a more comprehensive approach than merely relying on judicial discretion."[168]

The newly balanced 2005 formula aimed "[t]o protect consumers when a debtor proposes to sell their personal information."[169] The category of private information that the amendment aimed to protect was named Personally Identifiable Information (PII),[170] which was defined to include personal data such as first and last names, geographical or electronic addresses, telephone numbers, social security account numbers, or the account numbers of credit cards issued to individuals that provided data to the debtor subject to bankruptcy proceedings "in connection with obtaining a product or a service from the debtor primarily for personal, family, or household purposes."[171]

A three-pronged protection formula was introduced, to be resorted to in case the debtor, on the date of the commencement of the case, has express privacy policies that prohibit the sale or lease of private consumer information. Alternatively, as some authors suggest, prohibition of sales in certain situations might be implied as well if the debtor "fails to disclose

ruptcy Institute BI Law Review, Vol. 27, p. 7, also 1 Andrews Electronic Privacy Litig. Rep. 3, 1 NO. 3.

167 Tabb, J. C., 2020, p. 446.

168 Akselrad, M. R., 2021, p. 14.

169 Baxter, M. St. P., 2018, p. 3.

170 Bankruptcy Code section 101(41A).

171 Bankruptcy Code section 41(A)(A).

that the debtor may sell [private consumer information] to third parties."[172] The first prong of the test will only consider the sale of consumer privacy information to third parties if doing so is consistent with the debtor's data policies.[173] If such a policy exists or can be implied, then the second prong requires the appointment of a consumer privacy ombudsman[174] "to assist the court in its consideration of the facts, circumstances, and conditions of the proposed sale of PII,"[175] and to provide the court with pertinent information (usually by filing a report).[176] The third control mechanism is the bankruptcy court itself, which is entrusted with the responsibility to ensure that any sale would not violate "applicable nonbankruptcy law."[177]

The US's reliance on an ombudsman in the bankruptcy context is in and of itself interesting because "ombudsmanship" as a governmental institution was "invented" in Sweden after the deposition of their King in 1809, for tasks far removed from bankruptcy. In any event, the ombudsman approach described above may be useful for other countries pondering possible solutions to the mounting data privacy challenges cropping up in the context of insolvency law. Though, at least as the pertinent data from 2023 shows, the system has rarely been resorted to by consumers in the US, and "the law applies only to a subset of bankruptcy cases, and while the work of the ombuds may affect the sale of consumer data in those cases, legal protection is less than most would assume."[178]

The additional caveat, perhaps best demonstrated by the *UK Pacific Railway* case discussed above, is that the ombudsman is in itself additional red tape, and "because of the administrative costs to the bankruptcy estate of a consumer privacy ombudsman, debtors and creditors may not view

172 Baxter, M. St. P., 2018, p. 4.

173 Bankruptcy Code section 363(b)(1).

174 See Bankruptcy Code section 332, according to which a 'disinterested' third party is to be appointed as ombudsman by the United States trustee, upon order of the court, within 7 days "before the commencement of the hearing", at which the court will decide on sale or lease of consumer privacy information (as per section 363(b)(1)(B).

175 Baxter, M. St. P., 2018, p. 4.

176 *Ibid*. For illustration of such reports, see Baxter, M. St. P., 2018, notes 22–24, who himself has served in the capacity of a consumer privacy ombudsman. See, e.g., Second Report of Michael St. Patrick Baxter Consumer Privacy Ombudsman, p. 49, *In re Old BPS US Holdings, Inc.,* No. 16–12373 (Bankr. D. Del. 1. February 2017) in which the ombudsman was of the opinion that the sale proposed by the debtor was consistent with the existent privacy policy, if consumers were provided with notice on the transfer. *Ibid.*, Baxter, M. St. P., 2018, p. 5, note 23.

177 Bankruptcy Code section 363(b)(1)(ii).

178 Bradley, G. C., 2023, Privacy Theater in the Bankruptcy Courts, *Hastings Law Journal*, Vol. 74, Issue 3, p. 607.

the ombudsman's appointment to be in their interests and may have little incentive to favor such an appointment."[179] Even the scarce data on ombuds fees corroborate this,[180] notwithstanding that discounts in the fees or caps on the total fees seem to be quite common.[181] The average fees, expenses, and hourly fees of an ombudsman do also show that resorting to them is not cheap.[182]

5.4. US BANKRUPTCY–DATA PRIVACY CASES: CAPITA SELECTA

Although a detailed canvassing of what the US case law has to offer on the bankruptcy–data privacy interplay is beyond the scope of this article, a snapshot of a few cases is more than justified. While some US court cases resemble their European counterparts to various degrees, many revolve around quite different kinds of fact patterns and conclude with judgements founded upon distinct policies and legal positions. For example, the cases involving companies that gathered consumer "big data" seem to bring to the surface problems that have a lot in common with European ones, including major systemic questions, as was the case in the aforementioned *Toysmart* case.

Instances involving single individuals (as opposed to organizations) in possession of private data and in seemingly simpler fact scenarios have also been reported in greater numbers in the US compared to Europe (at least in English language). These US individual cases seem to have escaped the attention of comparative scholars, but both cases involving individuals and those involving organizations share a valuable characteristic: they both illustrate new challenges that bankruptcy law faces in all sorts of niches across the globe where modern bankruptcy laws are in place. A hopefully instructive selection ensues, though a systematized in-depth analysis thereof will be left for a later piece.

179 Baxter, M. St. P., 2018, p. 15.

180 According to Bradley's dataset, the largest ombuds fees – above $305,000. – were paid in the large case *In Re Borders Group, Inc.* [453 B.R. 477, Bankr. S.D.N.Y. 2011]. See Bradley, G. C., 2023, p. 643.

181 *Ibid.*, p. 643.

182 As Bradley put it, after the ombuds collect data, "[t]hey file a report and sometimes appear in court to answer questions. Then they file their fee application, obtain payment, and go about their business." In the dataset with 141 cases, the median total fees were $13,876.04, the median hourly rate was $474, the median hours spent by ombud 29.55 hours, as the median expenses amounted to $133.70 (Bradley, G. C., 2023, p. 643).

5.4.1. Big Data Cases

As well as the oft-cited 2000 *Toysmart* case, it is worth mentioning the more recent "big caliber" *Caesar's Entertainment* case,[183] which revolved almost exclusively around a "collection of aggregated personal and behavioral data on over forty-five million individuals."[184] The debtor was part of a corporate group running casinos that had amassed a debt load it could not handle, which led to another conglomerate acquiring it in a leveraged buyout in the aftermath of the 2008 Credit Crunch.

Big data entered the picture in the case because the group had launched the Total Rewards Program in 1998 whereby "Caesars would give away free meals, tickets, and other amenities to returning customers while receiving information on the customers, including their identity, preferences, travel history, and gambling patterns, all in the name of providing greater customer service."[185] By January 2015, when the largest unit of the group filed for Chapter 11 reorganization, proceedings with $18bn liabilities, their most valuable asset turned out to be the data collected through the Total Rewards Program. A dispute arose between the debtor's creditors and the group's parent company (which remained solvent) because the collected data (valued by creditors at $1bn) was transferred to the parent company before the bankruptcy was filed.[186]

More nuanced personal rights (biometric data)[187] were exposed in the bankruptcy case of the Illinois *Pay by Touch* company, which used to supply "the largest fingerprint scan system in Illinois," its finger-scan payment technology having been sold to about 400 supermarkets in the US, during the period from 2002 to the company's demise in 2008.[188] Although a considerable number of consumers was unwilling to pay and let the price be deducted from their checking accounts by merely placing their index-finger on the finger-scan at the POS (point-of-service),

183 *In re Ceasars*, 2015 U.S. Dist. LEXIS 137235, p. 10.

184 Akselrad, M. R., 2021, p. 17.

185 *Ibid*.

186 Zimmerman, A., 2016, Caesars Bankruptcy Examiner: Fraudulent Conveyance Damages Could Reach $5.1B, *Forbes,* 16 March, (https://www.forbes.com/sites/spleverage/2016/03/16/ceasars-bankruptcy-examiner-fraudulentconveyance-damages-could-reach-5–1b/#3b0fb3a143f9, 16. 10. 2023). Cited in M. R., 2018, note 104.

187 The Illinois Biometric Information Privacy Act defines biometric data to include "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." See 74 ILCS 14/10.

188 Garry, M., 2008, Biometric Payment Ends after Vendor Files Bankruptcy, in: *Supermarket News*, 31 March (https://www.supermarketnews.com/technology/biometric-payment-ends-after-vendor-files-bankruptcy, 7. 9. 2023).

thousands of consumers' biometric data became exposed during the *Pay by Touch*'s bankruptcy.[189] In fact, the threat that such data could be "sold, distributed, or otherwise shared through bankruptcy proceedings without adequate protections for Illinois citizens"[190] has led to the enactment of Illinois' Biometric Information Privacy Act.[191] The act imposes duties similar to those contained in the European GDPR on private entities in possession of biometric data.[192]

5.4.2. Cases Tackling Individuals' Privacy Rights in the Bankruptcy Context

The bankruptcy cases involving individuals also provide valuable insights into the complexities of the bankruptcy–data privacy interface. One line of cases that tackled the possibility of "expunging" otherwise public bankruptcy information (the US variant of the European "right to be forgotten") is illustrative of the myriad variations in which this seemingly simple issue may appear, some of which may not yet have even surfaced in Europe. As according to the Fair Credit Reporting Act[193] bankruptcy filings can be reported for no more than ten years on an individual's credit file, US discretion-based court decisions demonstrate how innovative courts can be, and it also shows that the degree of protection afforded to individuals can vary greatly. It should be noted here that according to some US scholars, the right to be forgotten is "un-American and in constant conflict with [US] constitutional principles,"[194] and US bankruptcy law does not nor is it intended to offer individuals "an opportunity to *restore* their financial reputation" in a manner analogous to the way in which the European right to be forgotten allows individuals to "repair" their reputation.[195]

The factual background of each case is also instructive. Thus, in the 2021 case *In Re Chapman*,[196] the expungement or sealing of bankruptcy

189 The case has become a complex bankruptcy case implicating the whole group that Pay by Touch was part of. See *In Re Solidus Network WL* 8462968 (2008).

190 *Heard v. Becton* 440 F.Supp. 3d 960 (2020).

191 74 ILCS 14, P.A. 95–994, eff. 10–3–08.

192 See, e.g., section 15 on retention, collection, and destruction of biometric data, making disclosure of a written policy on these duties.

193 Fair Credit Reporting Act, 15 U.S.C. Section 1681c(a)(1).

194 George, E. J., 2018, The Pursuit of Happiness in the Digital Age: Using Bankruptcy and Copyright Law as a Blueprint for Implementing the Right to Be Forgotten in the U.S., *Georgetown Law Journal*, Vol. 106, No. 3, pp. 905-[iii]t 923, p. 923.

195 *Ibid.*, p. 923.

196 *In Re Chapman* 2021 WL 1346046, 6+, Bkrtcy.E.D.Wis. Note that more grounds were advanced by the debtor in the case than the one highlighted above, though each was rejected.

data was requested by a mother whose daughter made three consecutive bankruptcy filings against her without informing her and without having received any "durable" power of attorney from her mother for the purposes of managing her finances. The mother learned about her bankruptcy case only when a social worker visited to inform her about the sheriff's pending sale of her house. The court did not find the records, which were open to the public, to be "scandalous or defamatory",[197] and thus rejected both requests.

In the recent case *In Re Ploetz*,[198] the debtor's requests to reopen his case, vacate his discharge, and expunge his records were rejected by the court "[b]ecause there [was] no indication in the record that his case was filed without his authorization or the filings were untrue."

Somewhat more nuanced responses were given by the courts in two earlier cases that found middle-ground solutions instead of decisively rejecting expungement outright. The solutions in those cases were arrived at without any statutory basis.[199] The fact patterns of the two cases were simple: in the 2001 case *In Re Buppelmann*,[200] the debtor's lawyer filed for bankruptcy by forging the client's signature, while in the 2009 case *In Re Joyce*,[201] the debtor asked for expungement (worded in the petition as a request "to vacate") because the public bankruptcy records were "damaging his ability to obtain credit and 'move along with his life,'" and also claiming losses arising from a "bogus loan", but otherwise accepting his listed debts. While in the latter case the court rejected the request because none of the losses were caused by fraud, in *Buppelmann*, the court ruled that the claimant "was entitled to relief, but not in nature of expungement of records of this fraudulent filing."[202] The remedy afforded to the debtor was a note on the bankruptcy records which was thought sufficient to alert those checking the docket and thereby to prevent negative consequences, with the note stating that "the dismissed case was the result of fraud committed by a party other than the debtor."[203]

---

197 As per §107(b)(2) regulating "public access to papers", "the bankruptcy court may ... (2) protect a person with respect to scandalous or defamatory matter contained in a paper filed in a case under this title."

198 *In Re Ploetz* 2022 WL 190429 (Bkrtcy.E.D.Wis.).

199 Sections 105 (equitable powers of the bankruptcy court) and 107(b) might have come into sight. See *In Re Buppelmann* 269 B.R. 341 (Bkrtcy.M.D.Pa. 2001), p. 341.

200 *In Re Buppelmann* 269 B.R. 341 (Bkrtcy.M.D.Pa. 2001).

201 *In Re Joyce* 399 B.R. 382 (Bkrtcy.D.Del. 2009), p. 385.

202 *In Re Buppelmann*, p. 341.

203 *In Re Chapman*, para 3, p. 9.

5.4.3. Providers of Privacy Rights-Related Services in Bankruptcy Proceedings

Another class of cases relates to the potential abuse of private data when various services are provided by external companies or agents in bankruptcy proceedings, i.e., in situations similar to the aforementioned 2016 German *Rockenhausen* case. The facts of the recent *In re Madison Square Boys & Girls Club, Inc.* case[204] are telling in that respect, because they foreshadow new scenarios in which third-parties provide various services in bankruptcy proceedings, a process in which personal data might end up being mishandled or abused.

The case concerned the work of *claims agents* who may be retained to assist court clerks for claims-processing in bankruptcy proceedings,[205] and who may be remunerated for those services. Problems can arise because claims agents may engage private third parties operating on a for-profit basis, in this case for the facilitation of claims-trading. In the case, the for-profit third party operated a claims-trading website and charged a commission under an agreement with the claims agent. Part of the agreement involved the synchronization of their platform's data with the court's, which resulted in the court data on bankruptcy being handed over to private parties. Although the contract was duly revealed to the court, the engagement of the claims agent under those terms was denied as that would have violated the Code of Conduct for Judicial Employees.[206]

What matters here, however, is that such engagements of private parties may generate similar concerns as the sale bulk data. Or worse, myriad abuses of "known unknowns" type: to wit, "risks which have not been resolved, but which we know are risks and which we know have yet to be resolved."[207]

---

204 Case # 22–10910, Southern District of New York. In the jurisdiction, retention of a claims agent is a requirement if the number of creditors or equity holders in a bankruptcy case is 250 or above. See also Jonathan Randles, Bankruptcy-Service Providers are Questioned over Deals with a Claims-Trading Startup, WSJ 25 Aug. 2022.

205 Claims agents may be retained based on 28 U.S.C. §156(c).

206 As claims-agents are the 'extended hands' of court clerks, the canon that a judicial employee should avoid impropriety and the appearance of impropriety in all activities applies also to them. The same applies to the canon that a clerk may collect only fees prescribed by law.

207 This epistemological digression on the classification of risks, allegedly stems from US Defense Secretary Donald Rumsfeld, according to Alastair Hudson, who used it together with the less problematic expression of 'known knowns' and the most 'dangerous' 'unknown unknowns' to describe financial risks related to the theme of the Banking Crisis of 2008. (Hudson, A., 2009, *The Law of Finance*, Mytholmroyd, Sweet & Maxwell, para. 32–02, p. 457).

5.4.4. European Data Protection Law Versus US-Style Discovery

US cases reveal yet another type of data protection–bankruptcy law interface: use of European data protection laws as a defense against the charge of failing to supply documents following a discovery order of a US court. In the illustrative civil case of *United States v. Pivaroff,*[208] launched to enforce federal tax liens and a related judgment against the defendants (Ivan and Gwendolyn and two entities controlled by them), the Blenheim Trust Company Ltd. seated in Guernsey, Channel Islands – which served as a trustee for Pivaroff – was ordered to produce certain documents by a US court. Blenheim, however, refused to do so by invoking European data protection regulations and the liability that may ensue for the failure to abide by the regulations. This claim was not accepted by the US court as the harm or prejudice to Blenheim Trust was not particularized as is required by US Federal Rules of Civil Procedure.[209]

Bankruptcy law came into the picture in the case because the counsel for Blenheim supplied documents on some relevant third parties in a redacted format – contrary to the request of the plaintiff. These third parties have "filed for bankruptcy protection" and were thus protected by the automatic stay provisions of the Bankruptcy Code.[210] The court held that "the discovery requests were not directed to stayed entities, and the fact that the documents contain factual information about stayed entities is not grounds to prevent discovery of information relevant and discoverable within the meaning of Fed. R. Civ P. 26(b)(1)."[211]

6. Middle Ground Jurisdictions

6.1. MIDDLE GROUND DATA PRIVACY LAWS AS NEW GLOBAL MODELS?

A quick glance at the data evidencing the heightened importance that data privacy law has gained globally within the past several decades reveals that there are now more models of data protection, and therefore no account of models of data protection is complete unless it sketches at least a brief account of all the major models. These models differ in many ways,

208 *United States v. Pivaroff*, No. 2:13-cv-01498-APG-PAL (26 August 2015, U.S. Dist.C. Nevada).

209 Fed. R. Civ. P. 26(c).

210 *US v. Pivaroff* – Order-and-Report and Recommendation for Contempt Proceedings, p. 3.

211 *Ibid.* The court held the Trust and its director in civil contempt and fined them $ 1,000.00 per day until the required documents were submitted to the judge *in camera.*

and not only in their approach to the bankruptcy–data protection interface. China, for example, although influenced by EU data protection law (lately by the GDPR), eventually opted for its own route, which in some respects constitutes a new version of the European solution better suited to the Chinese legal environment.

Besides China, Canada is another middle ground system,[212] differing from both the US and Europe but sharing some core features from both, though perhaps more its southern neighbor. In particular, while the EU law's aim is to "centrally supervise the private sector's use of personal data" in order to protect "dignity", "[i]n Canada, privacy protection is focused on individual autonomy through personal control of information."[213] As we know already, in the US, "privacy protection is essentially liberty protection, i.e., protection from government."[214]

From the perspective of the bankruptcy–data privacy interface, however, the crucial point is that the middle ground systems could equally come forward with telling cases that have not yet surfaced elsewhere, and both these fact patterns and the legal responses given thereto could also end up being instructive to others. Surveying the cautious yet unorthodox evolution of data protection law in China and its idiosyncratic interplay with their first-ever individual bankruptcy proceedings in the testing phase, and then contrasting that with the mature Canadian system, is an invaluable tool for grasping the complexities of the bankruptcy–data privacy interface.

6.2. CANADIAN PERSPECTIVES

The modern history of Canadian privacy law can be dated to the passage of the 1983 federal Privacy Act establishing the office of the Privacy Commissioner of Canada. Initially, however, the Commissioner's mandate was limited to overseeing the work of about 250 federal departments, agencies, and Crown corporations.[215] The Office's duties were extended to the private sector only with the Personal Information Protection and Electronic Documents Act (PIPEDA),[216] which was brought into force in several stages over the period from 2001 to 2004. Despite being a generally

212 See, e.g., Levin, A., Nicholson, M. J., 2005, Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground, *University of Ottawa Law & Technology Journal*, Vol. 2, No. 2, pp. 357–395.

213 *Ibid.*, abstract.

214 *Ibid.*

215 Office of the Privacy Commissioner Canada, A Guide for Individuals – Protecting your Privacy (2015), p. 4, (https://www.priv.gc.ca/media/2036/guide_ind_e.pdf, 7. 9. 2023).

216 S.C. 2000, c. 5.

applicable statute, PIPEDA is of importance for our discussion here because the federal Bankruptcy and Insolvency Act (BIA) "[gave] very little direction on the privacy rights of third party information on bankruptcy."[217] Back then, a Canadian author writing about PIPEDA referred to Canada's southern neighbor as a jurisdiction in which there was "significant legislative activity ... dealing with online privacy in general and the protection of personal information on bankruptcy in particular," triggered by a few cases in which problems were caused by the sale of customer databases in bankruptcy.[218]

The dynamics of data privacy law in Canada are also unprecedented. In particular, as Bill C-11 aimed to introduce significant changes to the domain but was ultimately not passed into law, it was swiftly substituted by Bill C-27 which introduced the texts of three act-proposals,[219] the fate of which remains undetermined as of the time of writing.[220]

The Canadian experiences are equally instructive and may be used as supplementary sources that could help predict other issues that may emerge on the interface between bankruptcy and data privacy in the future. For example, the issue that came up in the 2021 case *Holdings Co-Operative (Re)*[221] was whether the majority of members of a national cooperative had the right to obtain a list of the members accumulated over the years (along with their addresses, possibly also including their email addresses and telephone numbers) in order to assist in the process of successfully restructuring the cooperative and thereby ensuring its survival. Similarly, many of the scenarios in the case law mentioned throughout this article have also appeared North of the 48th parallel, often in differing guises.

6.3. CHINESE PERSPECTIVES

At the present, China has no law dealing specifically with the insolvency of individuals (in Europe: consumers), though its introduction is being debated by scholars and the policy is being studied by government-appointed reform commissions. China has major problems with the growing

217 Geist, M., 2002, p. 66.

218 *Ibid.*, p. 64.

219 The proposed acts are titled the Consumer Privacy Protection Act (CPPA), the Artificial Intelligence and Data Act (AIDA), and the Personal Information and Data Protection Tribunal Act. (https://www.parl.ca/Content/Bills/441/Government/C-27/C-27_1/C-27_1.PDF, 7 September 2023). The legislative process can be followed at: https://www.parl.ca/legisinfo/en/bill/44–1/c-27 (7 September 2023).

220 See LegisInfo webpage of the Parliament of Canada (https://www.parl.ca/legisinfo/en/bill/44–1/c-27, 9. 9. 2023).

221 *1077 Holdings Co-Operative (Re),* 2021 BCSC 42, 2021 CarswellBC 895 (2021). The court held that the request was premature. *Ibid.,* para. 102.

number of insolvent individuals[222] and a high number of no-asset cases. The corollary burning issue is data protection in the context of bankruptcy law, though data protection in general has become a matter of high priority in China only as of late. In their search for suitable models, Chinese lawmakers have relied heavily on the European compact data protection regulations. As noted in a recent publication, "the recently adopted Data Security Law, is quite similar to the GDPR and shows that the EU was arguably successful in its hope that the norms in the GDPR would become widely adopted around the world."[223] Nonetheless, it makes increasingly more sense to speak of a distinct Chinese model.

The heightened importance of privacy and data protection – which surfaced not only in the bankruptcy context but also in the online world – has been afforded recognition by the Chinese state in various forms. The new Chinese Civil Code of 28 May 2020,[224] for example, devotes six quite detailed provisions to it (Arts. 1034–1039), in Chapter VI entitled "Rights of Privacy and Protection of Personal Information",[225] which has led to more sector-specific regulations, in particular, the 2021 Data Security Law (promulgated on 10 June 2021),[226] applicable from 1 September 2021, and the Personal Information Protection Act (PIPL) (promulgated on 20 August 2021), which came into force on 1 November 2021. The first focused on data handling policies in general (e.g., data categorization, data risk controls, export controls with a view of creating an environment that does not thwart development of connected industries), and the latter on

222 Various regional courts have developed trial rules to deal with the mounting debts of a growing number of insolvent individuals, a crisis that has been exacerbated by the COVID-19 pandemic, such as the Implementation Opinions on the Liquidation of Personal Debt of the Dongying Intermediate People's Court of Shandong Province of 3 December 2020, or the Zhejiang Provincial Higher People's Court's "Guidelines for the Centralized Liquidation of Personal Debts of Zhejiang Courts". These *sui generis* court-made rules are applied by the affected courts notwithstanding that they are, strictly speaking, not primary sources of law. On these and other regional initiatives see Parry, R., Zhang, H., Fu, J., 2021, Personal Insolvency in China: Necessities, Difficulties, and Possibilities, *Brooklyn Journal of International Law*, Vol. 46, No. 2, pp. 517–571.

223 Tobin, O., 2021, Data Protection and the Growing Political Dimension, *Privacy & Data Protection* 22(1), pp. 7–8.

224 The English text of the Civil Code (http://www.npc.gov.cn/englishnpc/c23934/202012/f627aa3a4651475db936899d69419d1e/files/47c16489e186437eab3244495cb47d66.pdf, 1. 3. 2023).

225 Yu, L., Ahl, B., 2021, China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform, *Hong Kong Law Journal*, Vol. 51, p. 293.

226 The unofficial English translation of the act is available at: https://www.chinalawtranslate.com/en/datasecuritylaw/ (8. 9. 2023).

protection of personal data.[227] China has made significant advancements in the sphere of general data protection with unprecedented speed.

Data protection in the context of bankruptcy, however, has remained an unresolved problem, the severity of which is evidenced by the fact that some regional courts have been forced to venture as far as introducing pilot programs, curiously not based on statutory law but by coining regionally-applicable "rules", to tackle the issue.[228] The forerunner was the Shenzhen Zone, an economic success story rivalling that of Hong Kong's, which passed an instrument entitled "Shenzhen Zone Interim Rules for the Registration and Disclosure of Personal Insolvency Information" on 21 February 2022[229] and established a register as required by said Rules.

Otherwise, the problems that emerge in China are similar to those that have arisen in Europe and the US. Due to the increase in the importance of bankruptcy in China within a short period of time, these include also data protection concerns in the bankruptcy context, as well from big data concerns to proliferation of various software applications extending also to bankruptcy data of individuals. In Hong Kong, for example, the Do No Evil App, developed by a company called the Glorious Destiny, similarly to the abovementioned 2016 German case decided by the court in Rockenhausen, the company provided access to bankruptcy data of insolvency individuals (as well as to data related to linked litigation, criminal offenses and some company data). Furthermore, the investigation[230] showed that the individuals that the data concerned were not aware that data concerning them was public, and the data was often inaccurate and outdated.

Less is known about the handling of personal data in the bankruptcy of the first Chinese bike-sharing company (Yueqi Information Technology Company), which had collected some personal data of the system's users and thus the need to sell the data in the context of bankruptcy proceedings.

227 See, for example, One Trust Data Guidance (https://www.dataguidance.com/notes/china-data-protection-overview, 9. 9. 2023).

228 Kilborn, J. J., (2023, forthcoming) Law in Books versus Law in Action in the Landmark Shenzhen, China, Personal Bankruptcy Regime, *Emory Bankruptcy Developments Journal*, Vol. 40, No. 1. The article details the reasons, based on a few recent cases, why the new system fails to produce the proclaimed outcomes "standardized relief consistent with international best practices".

229 Shenzhen Zone Justice Bureau, Shenzhen Zone Interim Rules for the Registration and Disclosure of Personal Insolvency Information, (http://sf.sz.gov.cn/szsgrpcxxgkpt/xgzy/content/post_9528625.html, Chinese language, 7. 9. 2023).

230 See the Report of the Hong Kong Privacy Commissioner No. R13–9744, 13 August 2013, (https://www.pcpd.org.hk/english/enforcement/commissioners_findings/investigation_reports/files/R13_9744_e.pdf,7. 9. 2023). See also Gunasekara, G., 2021, Enforcement Design for Data Privacy: A Comparative Study, *Singapore Journal of Legal Studies*, No. 1, p. 32.

The case does show that the handling of and possible sale of personal data in bankruptcy proceedings had undoubtedly become an issue in China as well, moreover as early as in 2018.[231]

7. What Follows?

What the above elaboration shows is that bankruptcy law is increasingly being impacted by data protection law. The teething problems attendant to this interface seem to be more visible in Europe, as suggested by the cases discussed in this article. This, however, should not lead to the conclusion that the article's findings are of little or no relevance elsewhere. The sequitur is rather that insolvency practitioners have no other choice but to master and apply data protection laws, and courts ought to learn how to balance the competing – if not colliding – policies of bankruptcy and data protection laws while adjudicating disputes on this interface. The ultimate question concerns the reconcilability of the core policies and functions of bankruptcy and data protection laws. Satisfactory answers from policy makers, scholars, and other stakeholders are still lacking with regards to many of the issues unearthed, inter alia, in this paper.

Consequently, the question asked by Geist (is there a satisfactory answer to be found in the current law on the myriad burgeoning technology-driven questions and on the bankruptcy–data protection interface itself?) should be answered in the negative. This disappointing response applies even with regards to Europe's supposedly comprehensive model, which has proven to be the most influential model for a growing number of countries worldwide.

The reasons for this are twofold. On the one hand, the GDPR as the embodiment of Europe's comprehensive data protection regulation is a general code that does not contain provisions specifically targeting insolvency law, notwithstanding the quite intensive consultations that preceded the enactment of the 2015 Recast EIR. As one commentator stated, the GDPR risks becoming the "law of everything" because as new technologies emerge soon everything might contain personal data, triggering the application of the GDPR due to the open-ended reach of the key concept of "personal data".[232]

231 Zheng, C., 2018, Xiaoming court-ordered to refund bike deposits, *China Daily*, 23 March (https://global.chinadaily.com.cn/a/201803/23/WS5ab474bda3105cdcf6513d22.html, 9. 9. 2023).

232 Purtova, N., 2018, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, *Law, Innovation and Technology*, Vol. 10, No. 1, pp. 40–81.

On the other hand, the Recast EIR's short new data protection chapter, together with a few provisions scattered around the rest of the EIR, could be perceived only as a rudimentary first step towards a general response for tackling the challenges that the bankruptcy–data protection interplay generates. Thus, it would be desirable for the next version of the EIR to be drafted with greater attention not only to more precise rules on the rights and limitations of data subjects and other parties involved in bankruptcy proceedings, but also to the delicate public interest in obtaining valuable data in the course of bankruptcy proceedings.

It can also be concluded that European data protection and US data privacy laws are on partially divergent developmental trajectories. While this constellation inevitably leads to differing positions in many but not all situations, and the traditionally more restrictive European approaches tend to differ from less stringent US solutions, this observation applies across the board, i.e., not just with respect to the ill-fated history of the EU-US Data Protection Framework[233] (EU Privacy Shield) or the yet-to-be seen prospects of the enforceability of the GDPR's extraterritorial reach.[234] With a dose of simplification, it can be said that the EU seems to prioritize data protection law (though not expressly), while US law is "more understanding" of the need to ensure the efficiency of the bankruptcy law.

Notwithstanding the above, there is obviously room for further cross-fertilization of the developmental approaches on both sides of the Atlantic (and those applied elsewhere, too) as far as our topic is concerned, first and foremost because – as the above covered cases amply prove – the same problems crop up everywhere, albeit in different guises. Moreover, pertinent lines of jurisprudence slowly emerging from courts and data protection authorities in Europe have shown not only that the interface remains poorly understood, but also that the future development of the interplay between these two domains should not be left to sheer inertia, considering the very real conflicts that exist between these two

233 As the earlier EU-US frameworks have been demolished, the birth of a new one was announced by the EU in 2022 as follows: "On 25 March 2022, President von der Leyen and President Biden announced that they had reached an agreement in principle on a new EU-U.S. Data Privacy Framework. The framework will foster trans-Atlantic data flows and address the concerns raised by the Court of Justice of the European Union in the *Schrems II* decision of July 2020. Following that, the EU and US teams worked for many months to finalise the details of this agreement and translate it into a legal framework" (https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_6045, 7. 9. 2023).

234 Houser, K. A., Voss, G. W., 2018, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law and Technology*, Vol. 25, No. 1.

prestigious branches of law, a conflict perhaps best-illustrated by the *UK Pacific Railways* case above.

The ultimate lesson, however, should be clear: a willingness to confront the challenges corollary to the data privacy–insolvency interface should replace the previous habit of eschewing this (only seemingly) simple set of issues.

Bibliography

Books and Book Chapters

1. Beširević, V., A Short History of Brexit, in: Ilić, T., Božić, M. (eds.), 2020, *NOMOPHYLAX: Collection of Papers in Honor of Srđan Šarkić*, Belgrade, PFUUB & Službeni glasnik, pp. 621–645.
2. Beširević, V., The Constitution in the European Union: The State of Affairs, in: Dupeyrix, A., Raulet, G. (eds.), 2014, *European Constitutionalism. Historical and Contemporary Perspectives*, Brussels, Peter Lang, coll. Euroclio, pp. 15–35.
3. Bork, R., Zwieten, K. van, 2022, *Commentary on the European Insolvency Regulation*, 2nd ed., Oxford, OUP.
4. Bygrave, L., 2014, *Data Privacy Law*, Oxford, OUP.
5. Craig, P., Búrca, G. de, 2020, *EU Law – Text, Cases, and Materials*, 7th UK ed., Oxford, OUP.
6. Garner, B. A. (ed.), 2009, *Black's Law Dictionary*, Deluxe 9th ed. Eagan, West.
7. Goode, R., McKendrick, E. 2020, *Goode and McKendrick on Commercial Law*, 6th ed., London, Penguin.
8. Gullifer, L., Payne, J., 2020, *Corporate Finance Law – Principles and Policy*, 3rd ed., Oxford, Hart.
9. Hudson, A., 2009, *The Law of Finance*, Mytholmroyd, Sweet & Maxwell.
10. Messmann, S., Tajti, T. (eds.), 2009, *The Case Law of Central and Eastern Europe – Enforcement of Contracts*, Bochum, European University Press.
11. Noel, R. F., 1919, *History of Bankruptcy Law*. Washington, D. C., Chas. H. Potter & Co.
12. Regan, P. M., The United States, in: Rule, J. B., Greenleaf, G. (eds.), 2008, *Global Privacy Protection*, Cheltenham, Elgar.
13. Svetlicinii, A., Enforcement of Contracts in the Republic of Moldova: The Impact of a Slow Transition, in: Messmann, S., Tajti, T. (eds.), 2009, *The Case Law of Central and Eastern Europe – Enforcement of Contracts*, Vol. 1, Bochum, European University Press.
14. Tabb, J. C., 2020, *The Law of Bankruptcy*, 5th ed., St. Paul, West Academic.
15. Tajti, T., Article 78 – Data protection, in: Bork, Reinhard & van Zwieten, Kristin (eds.), 2022, *Commentary on the European Insolvency Regulation*, 2nd ed., Oxford, Oxford University Press.

16. Veder, M., Article 24 – Establishment of insolvency registers, in: Bork, R., Zwieten, K. van (eds.), 2022, *Commentary on the European Insolvency Regulation*, 2nd ed., Oxford, Oxford University Press.

Law Journal and Law Review Articles

1. Akselrad, M. R., 2021, The Liquidation of Data Privacy: How and Outdated Bankruptcy Code Threatens Consumer Information, *Boston College Intellectual Property & Technology Forum*, pp. 1–23.
2. Baumer, D. L., Earp, J. B., Poindexter, J.C., 2004, Internet Privacy Law: A Comparison between the United States and the European Union, *Computers & Security*, Vol. 23, Issue 5, pp. 400– 412.
3. Baxter, M. St. P., 2018, The Sale of Personally Identifiable Information in Bankruptcy, *American Bankruptcy Institute BI Law Review*, 27, pp. 1–15.
4. Bennett, S. C., 2012, The "Right to Be Forgotten": Reconciling EU and US Perspectives, *Berkeley Journal of International Law*, Vol. 30, Issue 1, pp. 161–195.
5. Bradley, C. G., 2023, Privacy Theater in the Bankruptcy Courts, *Hastings Law Journal*, Vol.74, Issue 3, p. 607.
6. Brimsted, K., Evans, T., 2019, Data subject access requests – Three Illuminating UK Cases, *Privacy & D.P.*, Vol. 19, No. 7, pp. 6–9.
7. Boyd, V., 2006, Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization, *Berkeley Journal of International Law*, Vol. 24, Issue 3, pp. 939–1008.
8. Búrca, G. de, 2013, After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?, *Maastricht Journal of European and Comparative Law*, 20, pp. 168–184.
9. Chander, A., Kaminski, M. E., McGeveran, W., 2021, Catalyzing Privacy Law, *Minnesota Law Review*, 105, pp. 1733–1802.
10. Cunningham, M., 2013, Diminishing Sovereignty: How European Privacy Law Became International Norm, *Santa Clara Journal of International Law,* 11, pp. 421–453.
11. Geist, M., 2002, When Dot-Coms Die: The E-Commerce Challenge to Canada's Bankruptcy Law, *Canadian Business Law Journal*, 37, pp. 34–74.
12. George, E. J., 2018, The Pursuit of Happiness in the Digital Age: Using Bankruptcy and Copyright Law as a Blueprint for Implementing the Right to Be Forgotten in the U.S., *Georgetown Law Journal*, Vol. 106, No. 3, pp. 905–932.
13. Greenleaf, G., Cottier, B., 2020, 2020 Ends a Decade of 62 New Data Privacy Laws, *Privacy Laws & Business International Report*, 163, pp. 24–26.
14. Gunasekara, G., 2021, Enforcement Design for Data Privacy: A Comparative Study, *Singapore Journal of Legal Studies*, 1, pp. 19–38.
15. Halberstam, D., 2015, It's the Autonomy, Stupid! A Modest Defense of Opinion 2/13 on EU Accession to the ECHR, and the Way Forward, *German Law Journal*, Vol. 16, Issue 1, pp. 105–146.

16. Houser, K. A., Voss, G. W., 2018, Gregory, GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law and Technology*, Vol. 25, No. 1.
17. Kilborn, J. J., (2023, forthcoming) Law in Books versus Law in Action in the Landmark Shenzhen, China, Personal Bankruptcy Regime, *Emory Bankruptcy Developments Journal*, Vol. 40, No. 1.
18. Kuijer, M., 2020, The Challenging Relationship between the European Convention on Human Rights and the EU Legal Order: Consequences of a Delayed Accession, *The International Journal of Human Rights*, Vol. 24, Issue 7, pp. 998–1010.
19. Levin, A., Nicholson, J. M., 2005, Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground, *University of Ottawa Law & Technology Journal*, Vol. 2, No. 2, pp. 357–395.
20. Moshell, R., 2005, ... And Then There Was One: The Outlook for a Self-Regulatory United States Amidst a Global Trend toward Comprehensive Data Protection, *Texas Tech Law Review* 37, pp. 357, 384.
21. Nicola, F. G., Pollicino, O., 2020, The Balkanization of Data Privacy Regulation, *West Virginia Law Review*, Vol. 123, Issue 1, pp. 61–116.
22. Parry, R., Zhang, H., Fu, J., 2021, Personal Insolvency in China: Necessities, Difficulties, and Possibilities, *Brooklyn Journal of International Law*, Vol. 46, No. 2, pp. 517–571.
23. Pernot-Leplay, E., 2020, China's Approach on Data Privacy Law: A Third Way between the U.S. and the EU? *Penn State Journal of Law & International Affairs*, Vol. 8, No. 1, pp. 49–117.
24. Piciocchi, C. *et al.*, 2018, Legal Issue in Governing Genetic Biobanks: The Italian Framework as a Case Study for the Implications for Citizen's Health through Public-Private Initiatives, *Journal of Community Genetics*, Vol. 9, Issue 2, pp. 177–190.
25. Purtova, N., 2018, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, *Law, Innovation and Technology*, Vol. 10, No. 1, pp. 40–81.
26. Reidenberg, J. R., 2001, E-Commerce and Trans-Atlantic Privacy, *Houston Law Review,* 38, pp. 717–749.
27. Salbu, S. R., 2002, The European Union Data Privacy Directive and International Relations, *Vanderbilt Journal of Transnational Law*, Vol. 35, Issue 2, pp. 655–695.
28. Schwartz, P. M., 2019, Global Data Privacy: The EU Way, *New York University Law Review*, 94, pp. 771–818.
29. Schwartz, P. M., Solove, D. J., 2014, Reconciling Personal Information in the United States and European Union, *California Law Review*, 102, pp. 877–916.
30. Shaffer, G., 2000, Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards, *Yale Journal of International Law,* Vol. 25, pp. 1–88.
31. Tajti (Thaythy), T., 2019, Unprotected Consumers in the Digital Age: The Consumer-creditors of Bankrupt, Abandoned, Defunct and of Zombie Companies, *Tilburg Law Review*, Vol. 24, Issue 1, pp. 3–26.
32. Tajti (Thaythy), T., 2017, Leasing in the Western Balkans and the Fall of the Austrian Hypo-Alpe-Adria Bank, *Pravni Zapisi*, Vol. VII, No. 2, pp. 155–221.

33. Tobin, O., 2021, Data Protection and the Growing Political Dimension, *Privacy & Data Protection* 22(1).
34. Ukrow, J., 2018, Practitioner's Corner – Data Protection without Frontiers? On the Relationship between EU GDPR and Amended CoE Convention 108, *European Data Protection Law Review*, Vol. 4, Issue 2, pp. 239–247.
35. Whitman, J. Q., The Two Western Cultures of Privacy: Dignity versus Liberty, *Yale Law Journal*, Vol. 113, No. 6, pp. 1151–1221.
36. Zeitzmann, S., 2021, The Council of Europe's Tromso Convention on Access to Official Documents, *European Data Protection Law Review,* 7, p. 232.
37. Yu, L., Ahl, B., 2021, China's Evolving Data Protection Law and the Financial Credit Information System: Court Practice and Suggestions for Legislative Reform, *Hong Kong Law Journal*, Vol. 51, pp. 287–308.

Industry Publications

1. EDPO, Brexit and the Data Protection Representative – What is the Impact for your Company? (https://edpo.com/uk-representative/, 7. 9. 2023).
2. Irish Consultative Committee of Accountancy Bodies, General Data Protection Regulation – Guidance for Insolvency Practitioners, Technical Release 02/2019, updated October 2022 (https://www.accaglobal.com/content/dam/ACCA_Global/Technical/insolv/GDPR%20Guidance%20for%20Insolvency%20Practitioners.pdf, 16. 10. 2023).
3. Rhodes, S.W., Bankruptcy Decisions on Privacy Issues, paper prepared for American Bankruptcy Institute 2003 Annual Spring Meeting (10–13 April 2003), ABI 557, para 11.

Legislation, Regulation, and Soft Law Instruments

Canada

1. The Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
2. Office of the Privacy Commissioner Canada, 2015, A Guide for Individuals – Protecting your Privacy, 4, (https://www.priv.gc.ca/media/2036/guide_ind_e.pdf, 16. 10. 2023)[pinyin: Minfadian].

China

1. Civil Code of the People's Republic of China 2020 (in force: 1 January 2021).
2. Data Security Act of the People's Republic of China 2021 (in force: 1 September 2021).
3. Personal Information Protection Law of the People's Republic of China (PIPL) 2021 (in force: 1 November 2021).
4. Justice Bureau of Shenzhen Municipality, Shenzhen Zone Interim Rules for the Registration and Disclosure of Personal Insolvency Information, (http://sf.sz.gov.cn/szsgrpcxxgkpt/xgzy/content/post_9528625.html, Chinese language, 16. 10. 2023).

5. Implementation Opinions on the Liquidation of Personal Debts (for Trial Implementation), promulgated by the Intermediate People's Court of Dongying City (effective 1 December 2020).
6. Zhejiang Provincial Higher People's Court, *Guidelines for the Centralized Liquidation of Personal Debts of Zhejiang Courts* (3 December 2020).

Council of Europe

1. Council of Europe, Convention 108: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, E.T.S. 108.
2. Council of Europe, CETS No. 223, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, 10 October 2018).
3. Council of Europe, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), CM(2018)2-final.

European Union

1. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regards to the processing of personal data and on the free movement of such data.
2. Council Regulation (EC) No. 1346/2000 of 29 May 2000 on Insolvency Proceedings, recast by Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings.
3. Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 (E-Privacy Directive), as amended by the EU telecoms reform package from November 2009.
4. Commission communication of 1st of October 2004 "Community guidelines on State aid for rescuing and restructuring firms in difficulty" (Official Journal 244, 1 December 2004, pp. 2–17).
5. Commission communication of 5 October 2007 "Overcoming the stigma of business failure – for a second chance policy – Implementing the Lisbon Partnership for Growth and Jobs" (COM/2007/0584 final).
6. Commission Communication of 25 June 2008: "Think Small First" – A Small Business Act for Europe (COM, 2008, 394 final)
7. Commission Recommendation of 12 March 2014 on a new approach to business failure and insolvency (L 74/65).
8. Charter of Fundamental Rights of the European Union, 2012/C 326/02.
9. Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the application of Council Regulation (EC) No. 1346/2000 of 29 May 2000 on insolvency proceedings (COM[2012] 743 final).
10. Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a Regulation amending Council Regulation (EC) No. 1346/2000 on insolvency proceedings, OJ C 358, 7 December 2013, pp. 15–16.

11. Regulation (EU) 2015/848 of the European Parliament and of the Council of 20 May 2015 on insolvency proceedings (recast).
12. 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).
13. Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, OJ L 295, 21 November 2018.
14. Directive (EU) 2019/1023 of the European Parliament and of the Council of 20 June 2019 on preventive restructuring frameworks, on discharge of debt and disqualifications, and on measures to increase the efficiency of procedures concerning restructuring, insolvency and discharge of debt, and amending Directive (EU) 2017/1132 (Directive on restructuring and insolvency).
15. Proposal for a Directive of the European Parliament and of the Council harmonising certain aspects of insolvency law, Brussels, 7 December 2022 COM(2022) 702 final 2022/0408 (COD).

OECD

1. OECD, Guideline Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), as updated in 2013.
2. OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, OECD/LEGAL/0188 (2022).

United Kingdom

1. Insolvency Act 1986, UK Public General Acts, 1986 c. 45.
2. The Data Protection Act, UK Public General Acts 2018 c. 12.

United States

Federal Level

1. The Privacy Act of 1974, as amended, 5 U.S.C. § 552a.
2. The Bankruptcy Reform Act of 1978 (Pub. L. 95–598, 92 Stat. 2549, November 6, 1978) – the Bankruptcy Code.
3. Bankruptcy Rule 2004.
4. 2005 Bankruptcy Abuse Prevention and Consumer Protection Act, Pub. L. No. 109–8, 119 Stat. 23 (2005).

State Level

California

1. California Consumer Privacy Act of 2018, Cal. Civ. Code §§ 1798. 100–199 (West 2021) (stepped into force Jan. 2020).

Illinois

1. Illinois' Biometric Information Privacy Act, 74 ILCS 14, P.A. 95–994, eff. 10 March 2008.

Case Law

Canada

1. *1077 Holdings Co-Operative (Re)*, 2021 BCSC 42, 2021 CarswellBC 895 (2021).

European Union

1. *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos [es], Mario Costeja González* (C 131/12) ECLI:EU:C:2014:317.
2. CJEU, *Schrems I* Case C-362/14.
3. CJEU, *Schrems II* Case C-311/18 (as of 16 July 2020).

Germany

1. BGH IX ZB 85/08 (5 February 2009).
2. *AG Rockenhausen*, Urt. V. 09 August 2016 Az 2C 341/16.

Hungary

1. Case NAIH-2087–5/2012/H (March 2012) (in Hungarian language).

Moldova

1. *Banca VIAS* 32760/04 (judgment delivered on 6 November 2007)
2. *Oferta Plus SRL* (14385/04 judgment delivered on 12 February 2008).

United Kingdom

1. *Re Southern Pacific Personal Loans Ltd*., [2013] EWHC 2485 (Ch).
2. *Oakley Smith v. Information Officer*, EWHC 2485 (Ch), 2013 WL 3994837 (2013).
3. *London Oil and Gas Ltd (In Administration)*, [2019] EWHC 3675.
4. *Green v SCL Group Ltd* [2019] EWHC 954 (Ch); [2019] B.P.I.R. 833; [2019] 4 WLUK 301 (Ch D).
5. *Dawson-Damer v. Taylore Wessing LLP*, [2020] EWCA Civ 352, 2020 WL 01158643.

United States

Federal Level

1. *Maxwell Communication Corp. v. Sociètè Gènèrale* 93 F.3d 1036 (US Court of Appeals, 2nd Cir., 1996).
2. *In re Toysmart.com Inc. LLC*, No. 00–13995 (Bankr. D. Mass., Aug. 17, 2000).

3. *In Re Solidus Network WL* 8462968 (2008).
4. *In Re Joyce* 399 B.R. 382 (Bkrtcy.D.Del. 2009).
5. *In re Ceasars*, 2015 U.S. Dist. LEXIS 137235.
6. *In Re Borders Group, Inc.* [453 B.R. 477, Bankr. S.D.N.Y. 2011].
7. *United States v. Pivaroff*, No. 2:13-cv-01498-APG-PAL (26 August 2015, U.S. Dist.C. Nevada).
8. *In re Old BPS US Holdings, Inc.*, No. 16–12373 (Bankr. D. Del. Feb. 1, 2017).
9. *Heard v. Becton* 440 F.Supp. 3d 960 (2020).
10. *In Re Chapman* 2021 WL 1346046, 6+, Bkrtcy.E.D.Wis.
11. *In Re Buppelmann* 269 B.R. 341 (Bkrtcy.M.D.Pa. 2001)
12. *In Re Ploetz* 2022 WL 190429 (Bkrtcy.E.D.Wis.).
13. *Federal Trade Commission v. Toysmart.com Inc.*, No. 00–11341-RGS (21 Aug. 2023).
14. *Chasom Brown, et al. v. Google LLC*, Case No: 4:20-cv-3664-YGR [US District Court, N.D. California, 7th Aug 2023].

State Level

1. *In Re Blackwell*, 263 B.R. 505 (W.D. Tex. 2000).

Internet Sources

1. Buyse, A., CJEU Rules: Draft Agreement on EU Accession to ECHR Incompatible with EU Law, *ECHR Blog* 2014/12/20 (blog text no longer available online as of 15 August 2022).
2. European e-Justice Portal, general information on insolvency law and insolvency registers of the Member States (https://e-justice.europa.eu/110/EN/bankruptcy_and_insolvency_registers, 16. 10. 2023).
3. Rosenkotter, E., Wutscher, M., 2022, Fifth State in the Union Becomes Fifth State to Enact Data Private Legislation, *InsideARM*, 17 May, (https://www.insidearm.com/news/00048260-fifth-state-union-becomes-fifth-state-ena/, 16. 10. 2023).
4. Scheinin, M., 2014, CJEU Opinion 2/13 – Three Mitigating Circumstances, *VerfBlog*, December 26, (http://www.verfassungsblog.de/cjeu-opinion-213-three-mitigating-circumstances/, 7. 9. 2023).
5. Zimmerman, A., 2016, Caesars Bankruptcy Examiner: Fraudulent Conveyance Damages Could Reach $5.1B, *Forbes*, 16 March, (https://www.forbes.com/sites/spleverage/2016/03/16/ceasars-bankruptcy-examiner-fraudulent-conveyance-damages-could-reach-5–1b/#3b0fb3a143f9, 16. 10. 2023).

Other Sources

1. Anonim., 2019, Facebook to pay $5bn fine to settle Cambridge Analytica claim – Case Comment, *Comp. & Risk* 8(4).

2. Garry, M., 2008 Biometric Payment Ends after Vendor Files Bankruptcy, *Supermarket News*, 31 March, (https://www.supermarketnews.com/technology/biometric-payment-ends-after-vendor-files-bankruptcy, 16. 10. 2023).
3. One Trust Data Guidance, 2023, China – Data Protection Overview, October, (https://www.dataguidance.com/notes/china-data-protection-overview, 16. 10. 2023).
4. Parliament of Canada, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (https://www.parl.ca/legisinfo/en/bill/44–1/c-27, 16. 10. 2023).
5. Zheng, C., 2018, Xiaoming court-ordered to refund bike deposits, *China Daily,* 23 March, (https://global.chinadaily.com.cn/a/201803/23/WS5ab474bda3105cdcf6513d22.html, 9. 9. 2023).

NOVA GRANICA: IZAZOVI RASTUĆEG UTICAJA PRAVA O ZAŠTITI LIČNIH PODATAKA NA STEČAJNO PRAVO

Tibor Tajti

APSTRAKT

Kako, na koji način i sa kojim posledicama pravo zaštite ličnih podataka (u Evropi: *data protection* – u SAD: *data privacy*) utiče na stečajno pravo pitanja su koja su ostala neobrađena i pored besprimernog značaja koji je pravo zaštite ličnih podataka dobilo u poslednje dve decenije kako u Evropi, tako i globalno. Pored opisa istorije i glavnih karakteristika regulative i problema između dveju grana prava, članak pokušava da nadopuni ovaj vakuum putem analize jednog broja sudskih odluka i odluka agencija za zaštitu ličnih podataka koje se bave pitanjima uticaja prava zaštite ličnih podataka na stečajno pravo. Analizirani slučajevi su prvenstveno iz Evrope, Sjedinjenih Država, kao i iz Kanade i Kine, kao primeri pravnih sistema koji su našli svoj specifičan model zaštite ličnih podataka.

Ključne reči: stečajno pravo, pravo zaštite ličnih podataka, Uredba Evropske unije o stečajnom postupku (prerađena verzija), e-Justice portal Evropske unije, spojeni stečajni registri, birokratija (red tape), pravni sistemi središnje orijentacije.

Article History:

Received: 13 September 2023

Accepted: 20 November 2023