DOI 10.5817/MUJLT2025-2-5

ON THE POSSIBLE USE OF DATABASES TO SECURE RECEIVABLE DEBTS *

by

MACIEJ BUJALSKI †

The article assesses the possibilities of using databases to secure receivable debts, i.e. as collateral, more than ten years after the ruling in the case Your Response v. Datateam Business Media where this possibility was denied. In order to do so, it first examines why someone may wish to use a database for this purpose and what the features are, including the limited accessibility of the database and its contents, that make a database an asset that may be useful in that context. The article then addresses the scope of the sui generis database right and its limited utility from the perspective of security rights, taking into consideration the entry into force of the Data Act. It analyses databases at three different levels: semantical, syntactical and structural, exploring at which level the features resulting in the value of the database should be placed, and thus the level at which the question of establishing a security interest over a database should be dealt with. The article goes on to provide for some theoretical approaches of introducing the rules on securities over databases into the legal system. It analyses the perspective of introducing proprietary rights to the database, the possible qualification of the database as a digital asset and the question of its control, as well as the contractual schemes that may be used in order to establish and enforce the security interest over a database.

* This paper is an element of the research carried out under the project 'Virtually secured credit? Security rights in digital goods' financed by Narodowe Centrum Nauki (NCN) [National Science Centre] in Krakow, Poland – number 2022/45/B/HS5/02952. It was presented in its initial shape at the Cyberspace conference held by Masaryk University in Brno on 29-30 November 2024. The author would like to acknowledge all the valuable comments he has received.

† Research Assistant in the Department of Comparative Private Law and PhD Candidate in the Doctoral School in the Social Sciences at the Jagiellonian University in Kraków, Poland. The author is supported by the Foundation for Polish Science (FNP), START 2025. E-mail: maciej.bujalski@uj.edu.pl; ORCID: 0000-0003-4004-8319

KEY WORDS
Database, Collateral, Security Rights, Digital Assets, Proprietary Rights to Data

1. INTRODUCTION
Although this article could possibly be regarded as another article on "data as the new oil", given its focus on the use of data – structured in the form of a digital database – and its market value and tradability, it approaches this issue from an angle that has not yet come under much scrutiny.[1] The paper addresses the use of databases to secure receivable debt.

The paper thus examines the possibility of establishing security interests over databases. Security interest – also referred to as "security" or "security right" – is understood as a way of granting a creditor an exclusive and preferential possibility to satisfy their claim against their debtor from the given object (the collateral), which is based on *in rem* rights to this object (broadly speaking, including not only instruments like pledges, but also the transfer of property made in order to secure the debt), which makes the security interest effective against third parties, including other creditors of the debtor.[2] The answer to the question of what can be used as collateral, i.e. as an object of security interest, varies across different jurisdictions. This paper will not delve into the specifics of these jurisdictions unless they serve as illustrative examples. Instead, it will focus on the conceptual possibility of using databases as collateral. It does not deal with the admissibility of such usage; rather, it outlines potential scenarios in which a database could serve as collateral, as well as risks that any prospective regulation should address. Thus, it is more of a law policy paper. However, there are some general preliminary concerns, noticeable through a brief comparative analysis, that need to be answered before a thorough examination of the security rights over databases can take place.

Yet, before launching a proper analysis on the use of databases as collateral, it is worth establishing why someone would want to use a database as collateral. The value comes from the specific features that may be associated with the database, and which result in its market value and make it useful as an object of security interest. Firstly, the stored information itself – the data – may present some value. Obtaining information costs money,

[1] The question was tackled over twenty years ago by Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), however, with the focus on IP rights and English law.

[2] Drobnig, U. (2012) Security Rights in Movable Assets. In: Jürgen Basedow, Klaus J. Hopt, Reinhard Zimmermann (eds.) *Max Planck Encyclopedia of European Private Law*. Oxford: Max-Planck-Gesellschaft, pt. 1. Available from: `https://max-eup2012.mpipriv.de/index.php/Security_Rights_in_Movable_Assets` [Accessed 28 December 2024].

and in this case one entity has already obtained it, so another does not need to. The information could be used for development purposes, or could be analysed in order to provide further data and information.[3] Secondly, the value may be linked to the fact that the data were already structured. Even if some information may be easily accessible, the fact that it is stored in some manner may be the source of added value. Thirdly, the value may result from the exclusive nature of the data stored in the database, or at least its limited accessibility.[4] The fact that only some entities may profit from the database in their business activity affects their competitiveness and makes databases an important asset. However, this feature challenges the use of a database as collateral, as its use in this way cannot result in making it available to the public, and there is a need for some guarantees that both parties will preserve this confidential-like nature of the database: the secured creditor for the duration of the security and the debtor right after enforcement. Those features need to be reflected in the legal means that allow databases to be used as collateral.

Those remarks are general ones as the databases in practice form a very heterogeneous group. For particular databases, the value and economic rationale of using them as collateral may be linked to specific features and uses of the database within the business activity of its holders. Some databases can bring benefits because access to them is subject to payable licences. Others contain some information that is difficult to collect, so their value reflects the costs that would have to be borne in order to form a parallel database (even though the data are available to the public, such as geological features). In other cases, the content of the database could be a large number of works protected by intellectual property rights, in which case the database reflects their value, which may well be higher than the sum of individual and non-structured copyrights. Such features may influence the individual decision of using a given database as collateral, or of specific arrangements relating to enforcement, which may sometimes require the transfer of intellectual property rights to the database contents, or consist of granting the creditor the benefits that the database produces. However, as tangible entities, all those databases are generally similar, in that they exist because of the code that provides their structure, as they can be accessed

[3] Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 9.

[4] See Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, p. 66.

and such access is generally limited for third parties,[5] and as they present the market value outlined above. That is why, even if not all databases could be used as collateral in practice, or if some present specific features that should be reflected in particular rules concerning such security interests (which is actually true for tangible objects as well), it is possible to distinguish databases as an object presenting certain common features making it possible to conceptualise the possibility of using them as security features.

Up to this moment, the term "database" could have been understood in the common and intuitive meaning. However, to answer the research question, the term "database" must be explained to establish the exact object that will be used as collateral. Therefore, the term "database" is generally used in this paper in a legally neutral and rather functional meaning. A suitably simple definition that may serve the further analysis can be found in the judgment of the Court of Appeal of England and Wales from 14 March 2014, rendered in the case *Your Response v. Datateam Business Media*, in which the court dealt with the possibility of using a digital database as collateral.[6] According to this definition, "the database consists of many individual pieces of information stored in a structured manner which renders them capable of systematic search and retrieval."[7] Hence, the database is a structured set of data that is capable of being analysed and which may present some market value because of its contents, structure and limited accessibility. As digital databases are the most commonly used, and as – given their size – they present significant economic value, they are the main interest of this paper. However, the considerations may also be related to traditional databases stored in certain tangible objects, such as ledgers.

The understanding of the term "database" is therefore similar to the definition resulting from Article 1(2) of Directive 96/9/EC on the legal protection of databases (Database Directive)[8] according to which a database is, for the purposes of this directive, a collection of independent works, data or other materials arranged in a systematic or methodical way and individually accessible by electronic or other means. However, the paper refrains from this definition as it has a strictly defined scope, excluding,

[5] Of course, a database may be publicly available. From an institutional point of view, it can still be used as security, though it does not represent the value for which someone would decide to use it that way.

[6] *Your Response Ltd v. Datateam Business Media Ltd* (2014) Court of Appeal, 3 WLR, p. 887. This judgement is commented on in detail in the further section.

[7] Your Response Ltd v. Datateam Business Media Ltd (2014). *op. cit.* p. 897, para. 28

[8] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (1996 L 77) 27 March. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A31996L0009` [Accessed 28 December 2024].

e.g. computer programs used in the making or operation of a database.[9] Meanwhile, for the purpose of analysing the possibilities of creating a security interest over a database, such limitations and distinctions are not needed as the structured set of data of certain value can be recorded in different forms, usually as a code, and those records are considered as possible collateral. Furthermore, this paper examines the security interests over a database as such and not over the *sui generis* database right under Article 7(1) of the Database Directive. Hence, relying on the definition of Article 1(2) of the Database Directive may be misleading since the term "database" would be read in the context of the *sui generis* database right. It is particularly important since this right has a limited scope of application making it of limited utility to be used as collateral. The reasons why the analysis should focus on the databases themselves serving as an object of security, and not the *sui generis* database right, are explained in the following section.

2. LEAVING THE *SUI GENERIS* DATABASE RIGHT ASIDE

The *sui generis* database right is an IP right entitling its holder to prevent third parties from extracting and re-using the contents of the database, and as such, like all IP rights, should be regarded as a proprietary right.[10] Therefore, it can be used as collateral, which should be regarded in the general context of securities established over IP rights.[11] The security interest over the *sui generis* database right can be established, for example, through a mortgage, pledge on rights or the proprietary transfer of the *sui generis* right.[12] However, the

[9] Recital 23 of the Database Directive.

[10] Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, pp. 51–52.

[11] See, in general, however without taking the *sui generis* database right into consideration, from the perspective of comparative law: Kieninger, E.-M. (2021) Security Rights in Intellectual Property. In: Katharina Boele-Woelki, Diego P. Fernández Arroyo, Alexandre Segenacnik (eds.) *General Reports of the XXth General Congress of the International Academy of Comparative Law*. Cham: Springer; and from the economic perspective: Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *GRUR International – Journal of European and International IP Law*, 73 (5). See also UNCITRAL (2011) *UNCITRAL Legislative Guide on Secured Transactions. Supplement on Security Rights in Intellectual Property*. Rome. Available from: `https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/10-57126_ebook_suppl_sr_ip.pdf` [Accessed 28 June 2025].

[12] Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), pp. 72, 75–81; Séjean, M. and Binctin, N. (2019) Sûretés Réelles Mobilières sur la Propriété Intellectuelle. *Revue Internationale de Droit Comparé*, 71 (2), pp. 447–450; Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, pp. 121, 152–153. See also, for other IP rights, Kieninger, E.-M. (2021) Security Rights in Intellectual Property. *op. cit.* pp. 353–358; Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *op. cit.* pp. 385–387.

idea behind protection with the *sui generis* database right under the Database Directive is not actually to protect the database as such, but to protect the investment made in order to create the database.[13] Thus, it is still an artificial construct of the *sui generis* right being an object of the security, and not the database itself, while what has the potential, analysed in this paper, is the actual database, being an electronic record containing a possibly valuable structured set of data. Consequently, it is the *sui generis* right that is subject to enforcement.[14] As a result, the secured creditor has no guarantee of the protection and confidentiality of the database contents. Even though the holder of the *sui generis* database right should generally have access to the database, it is possible that the creditor will be deprived of the real value of the database, whether through the denial of access to the database through technical barriers or because of the multiplication of the database contents and making them available to the public. Hence, the first reason why the analysis should not focus on the *sui generis* database right is the fact that it only reflects the actual database and aims at protecting the substantial investment made and not the contents of the database in which the real value lies. The second reason is the limited scope, both territorial and substantial, of application of protection under the Database Directive, which does not cover a vast number of databases presenting some significant value for which the *sui generis* database right cannot be used in order to constitute security.

It must be noted that the *sui generis* database right has limited territorial scope of application. It does not have its origin in international conventions, but it was the European Union's idea to promote innovation within Europe and to establish competitiveness with other regions.[15] As a result, Article 11 of the Database Directive allows the *sui generis* database right to be awarded only to those entities that are nationals of a Member State, have their habitual residence in the European Union or whose business activity presents a sufficient link with the territory of the European Union.[16] Even though the Database Directive allows the protection of databases whose makers are from third countries, under the condition of reciprocity,[17] similar intellectual

[13] Recital 40 of the Database Directive. See also Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia, p. 70.

[14] Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, p. 280.

[15] Recitals 11–12 of the Database Directive; Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, pp. 45–46; Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), p. 738.

[16] See Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar, p. 49.

[17] Recital 56 of the Database Directive. See also Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner

property rights to the *sui generis* database right are not harmonised globally and are rarely adopted in other jurisdictions.[18] The lack of reciprocal rights in some jurisdictions would make it impossible to enforce such a security. There is no point in establishing a security interest that would not enhance the creditor's position, as it could not be enforced. Furthermore, even though there are jurisdictions recognising a similar right, the use of the *sui generis* database right as collateral seems inefficient in international commerce, as it lacks the predictability sought by businesses.[19]

Furthermore, the *sui generis* database right does not cover many databases because of substantial reasons. It is mainly the question of the so-called "spin-off" theory due to which the datasets that are byproducts of the commercial activity, and not its purpose, cannot be protected with the *sui generis* database right.[20] The matter was further developed by the jurisprudence of the Court of Justice of the European Union, according to which the substantial investment in the creation of data is not sufficient to establish a *sui generis* database right, as the Database Directive sets as a condition for protecting the investment made in order to obtain already existing data.[21] Nowadays, the biggest concerns are databases containing machine-generated data, obtained by the producers of devices for everyday use – especially in the reality of the Internet of Things – through the sensors installed in these devices. Such data provides information not only on the user of the device, but also on many other external features and processes and hence has important market value for different kinds of entities. For example, in the automotive sector, the data obtained through car devices provides information not only about the driver's preferences, which may be

Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, p. 50.

18 Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), p. 739. However, similar rights were observed e.g. in Mexico, Russia or South Korea, see World Intellectual Property Organization (2002) *Summary on Existing Legislation Concerning Intellectual Property in Non-Original Databases*. SCCR/8/3. Geneva, p. 9. Available from: `https://www.wipo.int/edocs/mdocs/copyright/en/sccr_8/sccr_8_3.pdf` [Accessed 24 June 2025]; Doldirina, C. et al. (2016) Legal Approaches for Open Access to Research Data. *Law Archive Papers*, p. 20. Available from: `https://osf.io/preprints/lawarchive/n7gfa_v1` [Accessed 24 June 2024].

19 The risk was also observed by Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), pp. 84–85.

20 Derclaye, E. (2004) Databases Sui Generis Right: Should We Adopt the Spin Off Theory? *European Intellectual Property Review*, 26 (9), p. 402.

21 Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695, paras. 30–41; Judgment of 9 November 2004, Fixtures Marketing, C-338/02, EU:C:2004:696, paras. 24–37; Judgment of 9 November 2004, Fixtures Marketing, C-46/02, EU:C:2004:694, paras. 34–49; Judgment of 9 November 2004, Fixtures Marketing, C-444/02, EU:C:2004:697, paras. 40–53.

valuable for insurers, but also about traffic in general.[22] However, relying on the aforementioned jurisprudence and the "spin-off" theory, the scholarship, generally, opted for excluding such databases from the *sui generis* database rights' scope, under Article 7(1) of the Database Directive.[23] Since, in the case of databases containing machine-generated data, the producer makes a significant investment to produce a device that will allow the collection of data, the database itself is often a byproduct of the principal business activity. Seeing this tension, some authors argued for the shift in the interpretation or for the update of the Database Directive in order to grant such databases protection through the *sui generis* database right.[24] However, the European lawmaker took a different path and somehow cut off these debates.

The discussed datasets are mostly covered by Article 43 of the Data Act,[25] according to which the *sui generis* right provided for in Article 7 of the Database Directive shall not apply when data is obtained from or generated by a connected product or related service falling within the scope of the Data

[22] Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, p. 76.

[23] Zech, H. (2015) „Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. *Gewerblicher Rechtsschutz und Urheberrecht*, (12), pp. 1157–1158; Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 268; Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission, pp. 13–14; European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission, p. 20. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002` [Accessed 30 December 2024]; Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 14.

[24] See Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 27–30; Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5), pp. 743–744; European Commission (2022) *Study to Support an Impact Assessment for the Review of the Database Directive*. Final Report. Luxembourg: Publications Office of the European Union, pp. 52, 76–77. Available from: `https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act` [Accessed 30 December 2024]. Extensive interpretation was accepted in *Autobahnmaut* (2010) BGH, 25 March. (3) 2011 MMR, p. 188.

[25] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union* (L 2023/2854) 22 December. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32023R2854\&qid=1735552065097` [Accessed 30 December 2024].

Act. The provision – especially in the wording of the proposal[26] – raised doubts as to whether it is just an explanatory rule or the actual exclusion of the *sui generis* protection.[27] The purpose of this provision is to eliminate the risk that holders of data stored in databases would claim the *sui generis* right under Article 7 of the Database Directive and hinder the effective exercise of the right of users to access and use data, and the right to share data with third parties under the Data Act.[28] Thus, Article 43 of the Data Act should be regarded as providing for the general exclusion of the *sui generis* protection within the scope of the Data Act, which will grant at least some legal certainty.[29] It does not eliminate all the controversies, like the question on how to treat the databases containing two types of data, one protected by the *sui generis* database right, while the second are covered by the exclusion resulting from Article 43 of the Data Act.[30] However, the state of the art is that there are many databases of significant value – which was observed by the European lawmaker – that are not granted protection under the *sui generis* database right, but which the entity disposing of such a database may like to use it as collateral, for example in order to obtain funding for further development. Even though the holder of a database that is not covered by the Database Directive may benefit from other means of protection, e.g. contractual ones,[31] these limitations of the intellectual property rights to databases call for an alternative object of research.

---

[26] European Commission (2022) *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. COM(2022) 68 final. Brussels. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068` [Accessed 30 December 2024].

[27] See Drexl, J. et al. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. Max Planck Institute for Innovation and Competition Research Paper No. 22-05, pp. 91–96. Available from: `https://pure.mpg.de/rest/items/item_3388757_4/component/file_3395639/content` [Accessed 30 December 2024]; Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4), p. 230; Richter, H. (2024) Article 43 of the Data Act. In: Heinrich Amadeus Wolff, Stefan Brink, Antje v. Ungern-Sternberg (eds.) *BeckOK Datenschutzrecht*. 50th ed. München: C.H. Beck, pt. 19–22; Kim, D. (2024) Der Datenbankschutz sui generis nach dem Data Act. Having the cake and eating it too? *Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, MMR Appendix, pp. 88–89.

[28] Recital 112 of the Data Act.

[29] Richter, H. (2024) Article 43 of the Data Act. *op. cit.* p. 20. Whether the exclusion and not e.g. a specific fair use exception or free licensing scheme was the right approach to reach this aim is a separate question.

[30] *Op. cit.*, pt. 26–29; Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4), p. 230.

[31] See Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *Masaryk University Journal of Law and Technology*, 10 (2), pp. 182–183, with the reference to the Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10, para. 45.

Because of the limited scope of application of the *sui generis* database right, the focus on securities that may be established through this construct would lead to unjustified – from the market participants' and economic perspective – differentiation between various categories of databases that are economically suitable to be used as collateral. This perspective will not meet the possibilities that lie in this use of databases and so may be misleading.

All those arguments lead to the conclusion that the *sui generis* database right is of limited utility for the market players who would like to use a database as collateral. They wish to establish security over the database because of its structured content with the crucial role of access to it. Hence, there is a need to look for solutions that allow the establishment of a security interest over a database, understood as an electronic record, which is somehow a "tangible object" (though not in a legal sense). The following section assesses whether such solutions can be found in European legal orders. Then, the ways of establishing security over databases will be conceptualised at the theoretical level. However, it should be noted that the *sui generis* database right may play a supplementary role by granting measures of legal protection that may be associated with the models of establishing security interest over a database developed in the further sections.

3. COMPARATIVE LEGAL BACKGROUND

The comparative overlook of the possible use of databases as collaterals should begin with English law, where the question was directly dealt with more than ten years ago. It was the aforementioned ruling of the Court of Appeal of England and Wales in the case *Your Response v. Datateam Business Media*, in which the court denied the possibility of using a digital database as collateral.[32] The case was as follows: Datateam Business Media performed a contract to manage a digital database for the company called Your Response. When the latter did not pay the agreed fees, Datateam Business Media refused to release the database, and the information stored there was withheld until the full settlement was made. The court, therefore, had to examine whether a creditor with access to the debtor's database could withhold the database until the debt was paid – i.e. whether a creditor can exercise the "possessory lien" recognised under English law. This instrument is essentially equivalent to the civil law "right of retention" being a security, e.g. under French law.[33] Hence, the current state of the art under English law excludes qualifying databases as possible collaterals.

[32] Your Response Ltd v. Datateam Business Media Ltd (2014). *op. cit.* p. 887.
[33] Bourassin, M. (2024) *Droit des sûretés*. 8th ed. Paris: Lefebvre Dalloz, p. 575.

Therefore, two considerations of the court, when justifying its ruling, are worth re-examining as they illustrate the legal dilemmas that have to be addressed while proposing the framework for using databases as collaterals.

First, the court refused to accept that one can exercise possession over a digital database, being an intangible object, as possession is necessarily linked to physical control over an object and is an essential condition for a possessory lien.[34] However, the court also admitted that a digital database may be subject to control, even exclusive control, which is a broader concept than possession. Those issues are important, on the one hand, because possession is a condition for the effectiveness of many securities in various jurisdictions.[35] Therefore, if such a condition exists, it would be impossible to establish a security interest over a database. On the other hand, the strict position of the Court of Appeal of England and Wales may be considered as not adjusted to the digital reality surrounding us,[36] thus, maybe, possession should be succeeded by a more functional concept. Hence, in the model rules concerning the security rights in digital assets, the concept of control is used to replace "possession" in relation to those goods for which physical possession is hardly imaginable and would be somehow artificial.[37]

However, there are also alternative ways of establishing securities that are effective against third parties, particularly related to inscriptions in public registers.[38] French law may serve as an example. It provides for the establishment of security interests effective against third parties in two ways: through a transfer of possession or through an inscription in the register of movable securities.[39] Yet, it links the right to retention only with the

[34] Your Response Ltd v. Datateam Business Media Ltd (2014). *op. cit.* p. 895, para. 23.

[35] Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press, pp. 11–14.

[36] van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), pp. 245–246.

[37] See UNIDROIT (2023) *UNIDROIT Principles on Digital Assets and Private Law*. Rome, pp. 52–53. Available from: https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf [Accessed 28 December 2024]; European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna, pp. 20–21. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].

[38] Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press, pp. 10–11.

[39] Bourassin, M. (2024) Droit des sûretés. *op. cit.* p. 640.

securities established through a transfer of possession.[40] Furthermore, it recognises security interests that may be established over digital assets being "incorporeal movables" (*biens meubles incorporels*, Article 2355 of the French Civil Code), which category also includes digital assets (Article L.54-10-1 of the French Monetary and Financial Code). However, the mere possibility of such qualification of databases seems contestable as the notion aims to cover mainly cryptoassets.[41] So, establishing a security interest over a database is rather impossible under French law. However, even if accepted, the need to look for an alternative to the traditional concept of possession arises because of the need to ensure effective enforcement.[42]

Second, in the *Your Response v. Datateam Business Media* ruling, the court stated in a general manner that, *"whilst the physical medium and the rights [intellectual property rights – M.B.] are treated as property, the information itself has never been."*[43] The purpose of this paper is not to comprehensively deal with the question of proprietary rights to data, which has already been widely discussed in European legal scholarship[44] and somehow rejected

[40] Lisanti, C. and Pérechon, F. (2023) Le Nantissement d'Actifs Incorporels. *Revue des Procédures Collectives*, (3), p. 52.

[41] Julienne, M. (2020) Les Actifs Numériques, Entre Droit et Technologie. *Bulletin Joly Bourse*, (1), pp. 64–65. Extensively see Mekki, M. (2024) Actifs Numériques. In: *Répertoire de Droit Commercial*. Paris: Dalloz, pt. 36–65.

[42] Also Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2), pp. 82–83.

[43] Your Response Ltd v. Datateam Business Media Ltd (2014). *op. cit.*, p. 900, para. 42.

[44] See among many Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *GRUR International – Journal of European and International IP Law*, (10), pp. 880–884; Zech, H. (2016) A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice*, 11 (6), pp. 468–470; Drexl, J. et al. (2016) *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*. Max Planck Institute for Innovation and Competition Research Paper No. 16-10, pp. 2–3. Available from: `https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf` [Accessed 31 December 2024]; Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), pp. 272–278; Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 78–82; Zimmer, D. (2017) Property Rights Regarding Data? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 101–107; Banterle, F. (2018) The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *Sui Generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis. In: Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. Berlin: Springer, pp. 436–439.

by the European lawmakers in the Data Act,[45] which is not, however, free of controversies.[46] English law is also developing new approaches to proprietary rights in digital assets.[47] This paper will, however, take a stand in this discussion from the perspective of security rights – understood as *in rem* rights – which may provide some new arguments in this debate. It can be well observed in the context of German law that knows the narrow concept of thing (*Sache*), limited to the physical objects (§ 90 of the German Civil Code) and, thus excludes establishing the security over an electronic record, like database, that cannot be handed over (§ 1205 of the German Civil Code) and is not linked to any proprietary right.[48]

Therefore, a brief look into European jurisdictions proves that the regulations do not have much to offer to those wishing to establish a security over a database. However, the main issues that need to be addressed were properly identified over a decade ago in the *Your Response v. Datateam Business Media* ruling, and can serve as a starting point for further analysis. Yet, the search for solutions to fill these gaps should be preceded by explaining what should serve as an object of security in the proposed approaches to maintain clarity in legal analysis. For this purpose, three levels of database, being electronic records of structured datasets, should be outlined to establish the one with the value and features, making it important from the perspective of establishing a security interest. These are the semantic, syntactic, and structural levels, which will be explored in the following section.

---

[45] Graux, H. (2024) *What Is Data Ownership, and Does It Still Matter under EU Data Law?* Luxembourg: Publications Office of the European Union, p. 12. Available from: `https://data.europa.eu/sites/default/files/report/What\%20is\%20data\%20ownership\%2C\%20and\%20does\%20it\%20still\%20matter\%20under\%20EU\%20data\%20law.pdf` [Accessed 30 December 2024]; Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1), pp. 43–47. Available from: `https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf` [Accessed 4 July 2025]. See especially Recital 25 of the Data Act where it is stated that *"This Regulation should not be understood to confer any new right on data holders to use product data or related service data."*

[46] Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1), pp. 47–48. Available from: `https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf` [Accessed 4 July 2025], argues that it is possible to draw proprietary rights to data from the wording of the Data Act.

[47] See Calzolaio, E. (2023) Digital Assets and Property: Comparative Remarks from a Civil Law Perspective, *Comparative Law Review*, 14 (2), pp. 23–26.

[48] See Bülow P. (2019) Digitales Mobiliarpfandrecht. *Zeitschrift für Wirtschafts- und Bankrecht*, (25), pp. 1141–1145; Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, pp. 129–130.

4. THREE LEVELS OF A DATABASE

While analysing information from the perspective of private law and proprietary rights, three levels are distinguished. These are the semantic level – information with a certain meaning, the content of the information; the syntactic level – the signs and their relation with each other (it is therefore recorded information, though not necessarily having meaning); and the structural level – information contained in a certain physical carrier or, in a wider sense, information represented by the structure of a physical object capable of being subject to proprietary rights.[49] The same categorisation may be adjusted to databases.

At the semantic level of a database, there is information that results from the data constituting the database (and not from the database itself!). As indicated, this information can present some value, as it may be subject to analysis and interpretation. However, this information generally exists without a form of a database and should be regarded as publicly available, even though obtaining it may require costs from the person wanting to have access to the information.[50] The fundamental freedom of the right to information should therefore be placed at the semantic level.[51] This right cannot be restrained, so it is impossible to treat databases at the semantic level as an object to which certain rights are linked in the meaning of private law.[52] In some cases, the semantic level of information (more often than

[49] Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 194. This article summarizes the findings from Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck. See also Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.* p. 881, who distinguishes syntactic, semantic and pragmatic level and places data at the syntactic level.

[50] See also Catala, P. (1998) *Le Droit à l'Épreuve du Numérique*. Paris: Presses Universitaires de France, p. 244, who concludes that a person has the right to information that is available and allows them to create further information that may be subject to proprietary rights. The analysis was provided long before the division between the semantic and syntactic information was used in a legal context, but it may be regarded as being in common with these considerations as the "right to information" concerns the semantic level and the "information as a good" relates in some manner to the syntactic level.

[51] See Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 94–95, for whom the right to information may also concern the syntactic level.

[52] Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 443; Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196; Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 277; European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission, p. 34. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:`

the semantic level of databases) can be protected as an invention or a trade secret.[53] However, the semantic level of database is not – and it should not be – the most appropriate level for the purpose of securing the receivable debts.

Data are stored at the syntactic level, which makes a database a database. For digital databases – which are the main interest of this paper – the syntactic level is the one at which the database actually exists.[54] At this level, the semantical information is reflected with a code that set the datasets within a structure.[55] That way, the database, being an electronic record, is recognisable in the market. Since it is sufficiently specified and has economic value separate from its carrier, it can be qualified as a digital asset.[56] The code could be designed in such a way that the datasets cannot be retrieved, analysed or researched. However, it is generally designed in the opposite way, so that the database holder can benefit from it. This structure – existing because of the code – represents the value of the database.[57] The information stored could be used commercially because it presents the features of a systematic arrangement that can be subject to various operations enabling actual decisions or activities, e.g. to target a product to a specific market or to interact with a given customer due to the association of their preferences and contact details. Furthermore, it is at this level that the question of accessibility of the database is dealt with. As a result, it is the syntactic level that allows the holder to benefit from the content of the database, i.e. from the semantic level – lead market participants to perceive a database as having market value and thus being suitable for commercial use, including the establishment of the security interest.

52017SC0002 [Accessed 30 December 2024]. The Court of Appeal in *Your Response Ltd v. Datateam Business Media Ltd* (2014). *op. cit.* p. 900, para. 42 referred to this level of information.

53 Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), pp. 195–196; Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 263. Critically on the distinction between the semantic and syntactic information in the context of trade secrets protection Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, p. 68.

54 Zech, H. (2012) Information als Schutzgegenstand. Tübingen: Mohr Siebeck, p. 253.

55 Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 194. See, however, Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 361, where the author distinguishes structure of the database from the syntactic information as its content.

56 See van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), pp. 243–244, 251–252.

57 Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, pp. 319–320.

The last to explore is the structural level. For non-digital databases, the structural level can take the form of a file or – more probably – lots of files, being tangible objects and thus subject to proprietary rights. The question is more subtle with regard to digital databases. Firstly, one could argue that the servers on which the data are stored could be assigned to the structural level. As they can be owned and the right of ownership grants access to the stored data, they may be regarded as such.[58] However, the data can be removed from a given server, or the owner of the server may be denied access to its contents (though having access to the server as a tangible object). Secondly, it is possible to argue that the *sui generis* database right lies at the structural level.[59] This may be the case if the understanding of the structural level would be larger than referring only to tangible objects – as the case is at the moment.[60] The *sui generis* database right reflects the syntactical information contained in the database, but it does not aim to cover or protect it.[61] This right should be regarded as a *rei incorporalis*, and as such it grants the right-holder certain rights related to the database, effective against third parties, namely the right to prevent the contents of the database from being extracted or reused (Article 7(1) of the Database Directive).[62] Because of these features, the *sui generis* database right is actually similar to the right of ownership of a tangible object that is placed at the structural level but is only linked with the contents of this object (e.g. the fact that a page of a book was printed incorrectly does not affect the right of ownership of the book). However, as explained above, the *sui generis* database right is of limited utility from the perspective of establishing a security interest over a database.

---

[58] Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196.

[59] Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.*, pp. 881–882 places all the IP rights at the level of pragmatics.

[60] Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3), p. 196.

[61] Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck, p. 366. Similarly, for the copyrights, Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *op. cit.* pp. 881–882. See, however, Vivant, M. (2006) La Privatisation de l'Information par la Propriété Intellectuelle. *Revue Internationale de Droit Économique*, vol. XX (4), pp. 380–381, who argues that the *sui generis* database right protects precisely the content of the information.

[62] See Derclaye, E. (2021) The Database Directive. In: Irini Stamatoudi, Paul Torremans (eds.) *EU Copyright Law. A Commentary*. 2nd ed. Cheltenham–Northampton: Edward Elgar, pp. 234–237; Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz, pp. 560, 563–564. For more on the rights of the right-holder see: Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695, paras. 49–61; Judgment of 9 October 2008, Directmedia, C-304-07, EU:C:2008:552, paras. 35–53; Judgment of 3 June 2021, CV-Online Latvia, C-762-19, EU:C:2021:434, paras. 31–37.

These considerations can be summarised and illustrated by the following table:

Semantic level	**Syntactic level**	**Structural level**
Information with certain meaning. The intellectual content	Signs and their relationship with each other. Recorded information, not necessarily having a meaning	Information contained in a certain physical carrier or in a wider sense the structure of a physical object or a construct representing information
Mere data, particular information constituting database	The code reflecting the information stored, the database as such	The servers, the *sui generis* database rights

From the carried-out observation of databases at these three levels, it follows that not only their actual value lies at the syntactical level, but also precisely these features of databases that may lead businesses to use a database as collateral. Although there is actually no easy way to do so, this does not stop attempts to look for one.

5. ESTABLISHING AND ENFORCING THE SECURITY INTERESTS OVER DATABASES: CONCEPTUAL FRAMEWORK

The question of whether a database – its syntactical level – could be used as collateral is, at this very moment, a question of national law. Some jurisdictions may know the mechanisms allowing this to happen, while others may not and could possibly not want to recognise such rules. Existing rules were briefly discussed above. However, as mentioned, this paper does not aim to answer the question of such admissibility, but to provide for various legislative approaches that may be chosen to set a framework for the rules on securities established over databases.

The first approach that comes to mind in the context of *in rem* rights, such as security rights, is the question of establishing proprietary rights to a database. There are some points worth making here, even though, at the legislative level, the idea of proprietary rights to data has been abandoned. The discussion that took place mostly covered the question of data protection. In that it was argued that the proprietary rights are not needed to grant the sufficient level of protection and that, for example, the already existing regulation on trade secrets[63] could be regarded as a well-suited solution that also limits the means of protection to those data (datasets) that merit

[63] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *Official Journal of the European Union*, (2016 L 157) 15 June. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32016L0943` [Accessed: 9 January 2025].

protection.[64] However, the question of granting data with proprietary rights should not be limited to the issue of protection. The private law links many features with the proprietary rights, one of which, the fundamental one, is their effectiveness against third parties.[65] This feature also explains why the proprietary rights can be used to establish securities. The fact that protection may be granted through other means does not mean that some kind of subjective right will not be needed for other purposes. Of course, this cannot be the decisive argument in the discussion, though the perspective of other applications of the proprietary rights, including the establishment of a security interest, should be taken into consideration as well.

This paper focuses on databases – structured sets of data that can be retrieved and analysed – which are the potential objects of proprietary rights. These electronic records form the core of our discussion rather than mere data itself. Databases that consist of a given structure in which data are stored, a structure of limited accessibility, could be regarded as rival and excludable goods, making them more suitable as a subject of proprietary rights than the data as such.[66] To such databases, principles of specificity and publicity can be applied so they can be at least envisaged as the object of proprietary rights.[67] In some doctrinal categories, not generally reflected by the current legislation, databases – as the term is understood as a form of digital record

[64] See Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 71–72; Weber, R.H. (2017) Improvement of Data Economy through Compulsory Licenses? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 141–142. A more sceptical position was taken by Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4), p. 269.

[65] van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), p. 236.

[66] Data as such are regarded as non-rivalrous, but excludable or non-excludable, depending on the context. See van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6), p. 250; Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission, p. 46; Kerber, W. (2017) Rights on Data: The EU Communication 'Building a European Data Economy' from an Economic Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart, pp. 115–120; Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, p. 5. Available from: `https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital-assets-proprietary-rights-and-enforcement.pdf` [Accessed: 9 January 2025].

[67] van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *op. cit.* p. 239.

that, although capable of being multiplied, is observable as a tangible object – may be assigned to the group of *res digitales*.[68] Granting databases proprietary rights of any kind will include them in the well-established framework of *in rem* security rights that covers both their establishment (including their effectiveness against third parties) and enforcement. It will be possible to establish security without depriving the debtor of access and control over a database that may be necessary to pursue its business activity, e.g. in the form of the fiduciary transfer of such a right. Moreover, the very fact of the existence of an absolute right to an object guarantees, from the perspective of the legal system, greater stability of its value. However, as such a right would still be a conventional – maybe even artificial – construct, there is a risk that it may not be functional in practice. At the theoretical level, the proprietary right should grant a right-holder the right to access the database, though it is possible that a debtor, using simple technical measures, may restrain the creditor entitled to the right from it. A response to that risk may consist, in case of the databases stored with a blockchain technology, of using a smart contract to enforce the security. Another problem is related to the need to guarantee the limited accessibility of the database. For this purpose, apart from a contract on establishing the security interest over the database, certain clauses granting confidentiality may also be needed.

The second approach involves the inclusion of databases into the category of digital assets – deliberately avoiding the assignment of proprietary rights – and examining the possibility of applying the model rules on security interests over digital assets, i.e. the ELI Principles[69] and the UNIDROIT Principles,[70] to databases. The adopted definitions of digital assets differ from one another, though they are considered not to cover data or datasets.[71]

---

[68] The category of *res digitales*, existing alongside the traditional concepts of *res corporals* and *res incorporales*, was developed by Pałka, P. (2016) *Redefining 'Property' in the Digital Era. When Online, Do as the Romans Did*. EUI Working Paper LAW 2016/08, pp. 24–27. Available from: https://cadmus.eui.eu/bitstream/handle/1814/40366/LAW_2016_08.pdf?sequence=1&isAllowed=y [Accessed: 9 January 2025].

[69] European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].

[70] UNIDROIT (2023) *UNIDROIT Principles on Digital Assets and Private Law*. Rome. Available from: https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf [Accessed 28 December 2024].

[71] Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, p. 5. Available from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digi

It is worth exploring whether databases may be covered by those rules, as digital assets are generally regarded as electronic records presenting some features required by the model rules. A digital database usually takes the form of an electronic record. The problem lies in its features, particularly the capability of being subject to control (Principle 2(2) of the UNIDROIT Principles). The concept of control – being in some way equivalent to possession – concerns the factual abilities that a person has in relation to the given digital assets.[72] It was defined this way in Principle 6(1) of the UNIDROIT Principles, which provides for three abilities that characterise control. Those are: (i) the exclusive ability to prevent others from obtaining substantially all of the benefit from the digital asset; (ii) the ability to obtain substantially all of the benefit from the digital asset; and (iii) the exclusive ability to transfer those abilities to others and to the possibility of identifying an entity as having the mentioned abilities. The requirement of exclusivity is, however, relaxed in Principle 6(3) of the UNIDROIT Principles which provides for exceptions to this requirement if the digital asset or the relevant protocol or system limits the use of it and if the entity in control has agreed on sharing the ability referred to in Principle 6(1)(i) with others. The crucial question in the context of establishing the security rights over databases is how the database at its syntactic level could meet the criterion of exclusivity, and whether that is desirable. Firstly, databases are not necessarily designed to be exclusive assets, even if they present limited accessibility. Secondly, as mentioned, it may be beneficial for the debtor to maintain factual control over a database,[73] which can only be associated with granting control to the creditor, e.g. through the multiplication of the database or granting them additional access to the database. It requires rethinking whether granting exclusivity through technical means, e.g. by blocking access to the database in the event the obligation is not performed, when agreed that, for the duration of the security interest, both the debtor and creditor will have access to the

tal-assets-proprietary-rights-and-enforcement.pdf [Accessed: 9 January 2025]. In favour of including data into the category of digital assets: Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2), p. 9.

[72] UNIDROIT (2023). *op. cit.* p. 52; Julienne, M. and Palmieri, F. (2023) Contrôle, Propriété et Possession dans les Principes UNIDROIT Relatifs aux Actifs Numériques. *Revue de Droit Bancaire et Financier*, (4), pp. 57–58; Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*, pp. 6–7. Available from: https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital-assets-proprietary-rights-and-enforcement.pdf [Accessed: 9 January 2025].

[73] Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1), p. 76.

database, could be the solution covered by Principle 6(3) of the UNIDROIT Principles.[74] The more complex definition of digital assets was adopted in the ELI Principles. In this view, digital assets are records or representations of value that are intangible (only electronically stored), capable of being subject to a right of control, enjoyment or use, and transferable.[75] As explained, the databases often present the market value, and since the ELI Principles opt for wide and economic understanding of "value",[76] this condition is met. While requiring digital assets to be exclusively stored, displayed and administrated electronically, the ELI Principles indicate that it may happen through a database.[77] However, it should not be regarded as ruling out databases, understood in this paper as electronic records structuring datasets, as digital assets within the scope of the ELI Principles. The principles refer to databases as to the technical mean of storage, having, in this context, a different function. Yet, since the social media accounts, containing various type of data and features, are regarded as digital assets,[78] the same is for databases combining datasets in a structured manner via an electronic record. Therefore, taking the blackletters into consideration, as the concept of control under the ELI Principles is relaxed (in comparison to the UNIDROIT Principles) and the second criterion is limited to the factual possibility of accessing and enjoying the digital asset,[79] and as there should be no doubt that databases are tradable, qualifying databases as digital assets under the ELI Principles is not excluded.

Alternatively, one may argue that databases, as such, do not meet the requirements to be qualified as a digital asset in the meaning of the model rules, though it is possible to develop an access right (in the form of a code or a token) that could be qualified as a digital asset.[80] In this model, a database will not be regarded as an exclusive good, but such an access right will be, meaning that every entity having access to a database will have an individual asset over which they have exclusive control. Apart from the controversies of qualifying databases as digital assets, the plea against this second approach

[74] See UNIDROIT (2023). *op. cit.* p. 56, where it is stated that *"a person who has control may wish to share its abilities with one or more other persons for purposes of convenience, security, or otherwise"*.

[75] European Law Institute (2022). *op. cit.* pp. 18 – 19.

[76] European Law Institute (2022). *op. cit.* p. 19.

[77] European Law Institute (2022). *op. cit.* p. 17.

[78] European Law Institute (2022). *op. cit.* pp. 19 – 20.

[79] European Law Institute (2022). *op. cit.* p. 18.

[80] This idea was introduced during a meeting between the project team members and Matthias Lehmann, who took a strict interpretation of on the notion and criterion of exclusivity used in the UNIDROIT Principles because of its link to the *in rem* rights and *erga omnes* efficacy of the security rights. Introduction of the access right should be accompanied with amendments to the Database Directive that will make it clear that exercise of the access right is not an infringement to the IP rights under this directive.

may be the fact that the model rules address the rules on the enforcement of security rights only to the limited extent.[81] There is therefore a risk that the possibility of establishing security interests over a database will be purely theoretic, lacking any efficient mechanisms of granting a creditor their rights.

The third approach is based on certain contractual schemes that may serve the purpose of establishing a security interest over a database. It is, for example, possible that two parties will enter into a contract on rules of access to a database that also grants them technical means of access, such as a given access code, which creates a contractual right to a database.[82] Such a right could then be the object of a pledge (pledge on rights). It is also possible to imagine that a right of access will be linked to the *sui generis* database right, which is already, in some cases, used as collateral.[83] The contractual means are also important from the perspective of granting the confidentiality of the database and its content. It was admitted that – out of the scope of the Database Directive – it is possible to restrain others from accessing and using the database through the contractual means.[84] The same applies for the parties to a contract concerning the use of a database as collateral. However – and this is a general concern of all the considered contractual schemes – any kind of obligation would be binding only for the parties to a contract (*inter partes*). It means, on the one hand, that a breach of duty concerning the confidentiality of the database would only result in claims for damages against the liable party (but others will be able to legally access the contents of the database, which deprives it, at least partially, of value),[85] and, on the other hand, a contractual right of access to a database could only be enforceable against a given debtor. The use of contractual mechanisms in the context of security interests over databases is also possible in light of the views on treating data as a tradeable commodity.[86] The logical consequence of such a

[81] European Law Institute (2025) *ELI Principles and Guidance for Enforcement Against Digital Assets*. Vienna, p. 9. Available from: `https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf` [Accessed 24 June 2024]. See also Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2), p. 78.

[82] Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia, p. 59; Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz, p. 565.

[83] Ferling, M. (2023). *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck, p. 155.

[84] Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10, para. 45.

[85] Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *op. cit.* p. 189; Zech, H. (2016) Data as a Tradeable Commodity. *op. cit.* p. 60.

[86] See in that matter De Franceschi, A. and Lehmann, M. (2015) Data as Tradeable Commodity and New Measures for their Protection. *The Italian Law Journal*, 1 (1), pp. 54–63; Zech, H. (2016) Data as a Tradeable Commodity. *op. cit.* pp. 52–61; American Law Institute and

stand is that also databases should be regarded as such. Hence, it could be possible that the enforcement of a security interest established over a database will consist of the transfer of the database to a creditor – which may be, for example, associated with the use of a smart contract – who will be also able to sell it further on the market, if the creditor does not personally have an interest in accessing the given dataset.

With regard to enforcement, in addition to the possibility of the creditor taking over the database (and/or rights associated with it) – to be used or sold – it is worth mentioning another method of enforcement that could be integrated into all three approaches. The debtor can often make the database available to other entities under a licensing model and base on this the business model. Then, the real benefit of the database is the licence fee (such a licence may or may not be a licence in the sense of intellectual property law – it depends on the object of the contract). The secured creditor's interest may, therefore, be satisfied if they are entitled to collect these benefits, for which they do not have to take over the database at all (and it may even be in their favour that it is the debtor who continues the business). This means that the enforcement of the security interest over a database may happen through such benefits, which in civil law terms would be regarded as fruits from the database (the proposed construction would be thus similar to the traditional institution of the *antichresis*).[87] Linking the enforceability of such benefits to the security interest established over a database allows the creditor to be satisfied from an abstract category for which the variability of the individual fees included in it is irrelevant. This is an important convenience in view of another construction that allows a creditor to be satisfied from such fees, i.e. the security interest created over the debtor's claims, which requires that every specific claim for a given fee be identified and indicated each time, including the entity obliged to satisfy it.

From the perspective of searching for legislative solutions there is not an easy choice, as all the approaches present some shortcomings. The main concerns that such a regulation has to address can be pointed out. They include, firstly, the actual access to the database, both for the creditor – in the event of non-performance – and for the debtor – while performing their obligation, which will allow them to pursue their activity. Secondly, there

European Law Institute (2023) *ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights*, p. 18. Available from: `https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy.pdf` [Accessed: 10 January 2025].

87 See Żok, K. (2020) Zastaw Antychretyczny – Zagadnienia Konstrukcyjne. In: Karol Szadkowski, Krzysztof Żok (eds.) *Zabezpieczenia Wierzytelności*. Warszawa: Wolters Kluwer, pp. 93–99; Verhagen, H.L.E. (2022) *Security and Credit in Roman Law*. Oxford: Oxford University Press, pp. 257–268.

is the question of granting confidentiality and limited accessibility to the database, both before enforcing the security interest – in the interest of the debtor – and after the enforcement – in order not to deprive the value that the database presents for the secured creditor.

6. CONCLUSION

This article addresses the possible use of databases in order to secure receivable debts. The paper outlines the market utility of databases for this purpose, which is linked to their value and lies in three features: in the content of the database, in the structure that makes a database suitable for exploitation (rather than a pure set of information) and in the exclusive nature, or rather limited accessibility, of the database. The legal mechanisms concerning the use of databases as collaterals should take these features into consideration in order to guarantee that a security right will be established over a database as such, and will grant the secured creditor access to an asset of real value. Hence, if choosing from the three levels, it is the syntactical level of the database that should be regarded as the proper object of the security rights. To this level, containing the code resulting in the structured sequence of signs, should be assigned the actual ability to benefit from the database, as well as to exclude others from doing so. Because of that – as well as because of the latest legal developments in the European Union, i.e. the Data Act – the *sui generis* database right under Article 7(1) of the Database Directive is not a sufficient legal concept from the perspective of security interests established over databases. At a general level, this raises questions about the rationale for introducing and preserving the *sui generis* database right, particularly if it lacks commercial value even for the applications examined in this article.

For now, there are no specific legal regulations on the use of databases as collateral. The possibility depends on national legal solutions, but mostly on the concept of a good accepted in a given jurisdiction. However, from a comparative perspective, European private law lacks legal instruments for establishing security interests over databases. Therefore, theoretical proposals were developed to address this issue. Three approaches to this question were considered. Each of them presents some advantages and disadvantages and merits further examination in relation to a particular legal system. The first consists of (re)opening discussion on the proprietary rights in databases – accompanied by the view that the subjective right guarantees certainty from the perspective of the legal system. The second aims at including databases into the category of digital assets for which the model laws on security rights are now being developed. The third, the softest one, is based on the application of certain contractual schemes. The future

regulation, if a lawmaker of any level decides to provide for one, should preserve the features that make a database a valuable asset. One general conclusion is that, as long as data and databases present a market value, which is rather beyond doubt, their possible market applications may be varied in nature and so should not be limited to issues of protection or trading but also cover their use in order to secure a transaction.

LIST OF REFERENCES

[1] Alejandre, G.M. (2021) Ownership of Databases: Personal Data Protection and Intellectual Property Rights on Databases. *European Review of Private Law*, 29 (5).

[2] American Law Institute and European Law Institute (2023) *ALI-ELI Principles for a Data Economy: Data Transactions and Data Rights*. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ALI-ELI_Principles_for_a_Data_Economy.pdf [Accessed: 10 January 2025].

[3] Aplin, T. (2017) Trading Data in the Digital Economy: Trade Secrets Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[4] *Autobahnmaut* (2010) BGH, 25 March. (3) 2011 MMR, p. 188.

[5] Banterle, F. (2018) The Interface Between Data Protection and IP Law: The Case of Trade Secrets and the Database *Sui Generis* Right in Marketing Operations, and the Ownership of Raw Data in Big Data Analysis. In: Mor Bakhoum, Beatriz Conde Gallego, Mark-Oliver Mackenrodt, Gintarė Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law*. Berlin: Springer.

[6] Bourassin, M. (2024) *Droit des sûretés*. 8th ed. Paris: Lefebvre Dalloz.

[7] Bujalski, M. (2025) Czy prawo francuskie może stanowić wzór dla regulacji realizacji zabezpieczeń na dobrach cyfrowych? *Forum Prawnicze*, 86 (2).

[8] Bülow P. (2019) Digitales Mobiliarpfandrecht. *Zeitschrift für Wirtschafts- und Bankrecht*, (25).

[9] Calzolaio, E. (2023) Digital Assets and Property: Comparative Remarks from a Civil Law Perspective, *Comparative Law Review*, 14 (2).

[10] Calzolaio, E. (2024) From data property to data access and back again? Comparative remarks on the EU Data Act. *Iceonline*, (1). Available from: https://www.lceonline.eu/wp-content/uploads/2024/04/I.03-Calzolaio.pdf [Accessed 4 July 2025].

[11] Catala, P. (1998) *Le Droit à l'Épreuve du Numérique*. Paris: Presses Universitaires de France.

[12] De Franceschi, A. and Lehmann, M. (2015) Data as Tradeable Commodity and New Measures for their Protection. *The Italian Law Journal*, 1 (1).

[13] Derclaye, E. (2004) Databases Sui Generis Right: Should We Adopt the Spin Off Theory? *European Intellectual Property Review*, 26 (9).

[14] Derclaye, E. (2008) *The Legal Protection of Databases. A Comparative Analysis*. Cheltenham–Northampton: Edward Elgar.

[15] Derclaye, E. (2021) The Database Directive. In: Irini Stamatoudi, Paul Torremans (eds.) *EU Copyright Law. A Commentary*. 2nd ed. Cheltenham–Northampton: Edward Elgar.

[16] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases. *Official Journal of the European Union* (1996 L 77) 27 March. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A31996L0009 [Accessed 28 December 2024].

[17] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. *Official Journal of the European Union* (2016 L 157) 15 June. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32016L0943 [Accessed: 9 January 2025].

[18] Doldirina, C. et al. (2016) Legal Approaches for Open Access to Research Data. *Law Archive Papers*. Available from: https://osf.io/preprints/lawarchive/n7gfa_v1 [Accessed 24 June 2024].

[19] Drexl, J. et al. (2016) *Data Ownership and Access to Data. Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*. Max Planck Institute for Innovation and Competition Research Paper No. 16-10. Available from: https://www.ip.mpg.de/fileadmin/ipmpg/content/stellungnahmen/positionspaper-data-eng-2016_08_16-def.pdf [Accessed 31 December 2024].

[20] Drexl, J. (2017) Designing Competitive Markets for Industrial Data – Between Propertisation and Access. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 8 (4).

[21] Drexl, J. et al. (2022) *Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. Max Planck Institute for Innovation and Competition Research Paper No. 22-05, pp. 91–96. Available from: https://pure.mpg.de/rest/items/item_33

88757_4/component/file_3395639/content [Accessed 30 December 2024].

[22] Drobnig, U. (2012) Security Rights in Movable Assets. In: Jürgen Basedow, Klaus J. Hopt, Reinhard Zimmermann (eds.) *Max Planck Encyclopedia of European Private Law*. Oxford: Max-Planck-Gesellschaft. Available from: https://max-eup2012.mpipriv.de/index.php/Security_Rights_in_Movable_Assets [Accessed 28 December 2024].

[23] Duch-Brown, N., Martens, B. and Mueller-Langer, F. (2017) *The Economics of Ownership, Access and Trade in Digital Data*. JRC Digital Economy Working Paper No. 2017-01. Seville: European Commission.

[24] European Commission (2017) *Commission Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy*. SWD(2017) 2 final. Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017SC0002 [Accessed 30 December 2024].

[25] European Commission (2022) *Study to Support an Impact Assessment for the Review of the Database Directive. Finał Report*. Luxembourg: Publications Office of the European Union. Available from: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act [Accessed 30 December 2024].

[26] European Commission (2022) *Proposal for a Regulation of the European Parliament and of the Council on Harmonised Rules on Fair Access to and Use of Data (Data Act)*. COM(2022) 68 final. Brussels. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0068 [Accessed 30 December 2024].

[27] European Law Institute (2022) *ELI Principles on the Use of Digital Assets as Security*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Principles_on_the_Use_of_Digital_Assets_as_Security.pdf [Accessed 28 December 2024].

[28] European Law Institute (2025) *ELI Principles and Guidance for Enforcement Against Digital Assets*. Vienna. Available from: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Projects/Access_to_Digital_Assets/ELI_Principles_and_Guidance_for_Enforcement_Against_Digital_Assets.pdf [Accessed 24 June 2024].

[29] Ferling, M. (2023) *Digitale Information als Kreditsicherheit*. Tübingen: Mohr Siebeck.

[30] Graux, H. (2024) *What Is Data Ownership, and Does It Still Matter under EU Data Law?* Luxembourg: Publications Office of the European Union. Available from: https://data.europa.eu/sites/default/files/report/What\%20is\%20data\%20ownership\%2C\%20and\%20does\%20it\%20still\%20matter\%20under\%20EU\%20data\%20law.pdf [Accessed 30 December 2024].

[31] Heller, D., Leitzinger, L. and Walz U. (2024) Intellectual Property as Business Loan Collateral: A Taxonomy of Institutional and Economic Determinants. *GRUR International – Journal of European and International IP Law*, 73 (5).

[32] Hugenholtz, P.B. (2017) Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[33] Judgment of 9 November 2004, British Horseracing, C-203/02, EU:C:2004:695.

[34] Judgment of 9 November 2004, Fixtures Marketing, C-338/02, EU:C:2004:696.

[35] Judgment of 9 November 2004, Fixtures Marketing, C-46/02, EU:C:2004:694.

[36] Judgment of 9 November 2004, Fixtures Marketing, C-444/02, EU:C:2004:697.

[37] Judgment of 9 October 2008, Directmedia, C-304-07, EU:C:2008:552.

[38] Judgement of 15 January 2015, Ryanair, C-30/14, EU:C:2015:10.

[39] Judgment of 3 June 2021, CV-Online Latvia, C-762-19, EU:C:2021:434.

[40] Julienne, M. (2020) Les Actifs Numériques, Entre Droit et Technologie. *Bulletin Joly Bourse*, (1).

[41] Julienne, M., Palmieri, F. (2023) Contrôle, Propriété et Possession dans les Principes UNIDROIT Relatifs aux Actifs Numériques. *Revue de Droit Bancaire et Financier*, (4).

[42] Kerber, W. (2017) Rights on Data: The EU Communication 'Building a European Data Economy' from an Economic Perspective. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[43] Kieninger, E.-M. (2004) Introduction: Security Rights in Movable Property within the Common Market and the Approach of the Study. In: Eva-Maria Kieninger (ed.) *Security Rights in Movable Property in European Private Law*. Cambridge: Cambridge University Press.

[44] Kieninger, E.-M. (2021) Security Rights in Intellectual Property. In: Katharina Boele-Woelki, Diego P. Fernández Arroyo, Alexandre Segenacnik (eds.) *General Reports of the XXth General Congress of the International Academy of Comparative Law*. Cham: Springer.

[45] Kim, D. (2024) Der Datenbankschutz sui generis nach dem Data Act. Having the cake and eating it too? *Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, MMR Appendix.

[46] Leistner, M. (2017) Big Data and the EU Database Directive 96/9/EC: Current Law and Potential for Reform. In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[47] Le Tourneau, P. (2022) *Contrats du Numérique*. 12th ed. Paris: Dalloz.

[48] Lipton, J.D. (2001) Security Interests in Electronic Databases. *International Journal of Law and Information Technology*, 9 (1).

[49] Lisanti, C. and Pérechon, F. (2023) Le Nantissement d'Actifs Incorporels. *Revue des Procédures Collectives*, (3).

[50] Mekki, M. (2024) Actifs Numériques. In: *Répertoire de Droit Commercial*. Paris: Dalloz.

[51] Myška, M. and Harašta J. (2016) Less Is More? Protecting Databases in the EU after Ryanair. *Masaryk University Journal of Law and Technology*, 10 (2).

[52] Nekit, K. (2024) The (Im)Possibility of Personal and Industrial (Machine-generated) Data to Be Subject to Property Rights. *International Journal of Law and Information Technology*, 32 (2).

[53] Pałka, P. (2016) *Redefining 'Property' in the Digital Era. When Online, Do as the Romans Did*. EUI Working Paper LAW 2016/08. Available from: `https://cadmus.eui.eu/bitstream/handle/1814/40366/LAW_2016_08.pdf?sequence=1\&isAllowed=y` [Accessed: 9 January 2025].

[54] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union* (L 2023/2854) 22 December. Available from: `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX\%3A32023R2854\&qid=1735552065097` [Accessed 30 December 2024].

[55] Richter, H. (2024) Article 43 of the Data Act. In: Heinrich Amadeus Wolff, Stefan Brink, Antje v. Ungern-Sternberg (eds.) *BeckOK Datenschutzrecht*. 50th ed. München: C.H. Beck.

[56] Rodríguez de las Heras Ballell, T. (2024) The Emergence of Principles and Best Practices on Digital Assets: Proprietary Rights, and Enforcement. *European Journal of Risk Regulation*. Available from: `https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B4DE880068B9292E7F2164715827067C/S1867299X24000552a.pdf/the-emergence-of-principles-and-best-practices-on-digital-`

assets-proprietary-rights-and-enforcement.pdf [Accessed: 9 January 2025].

[57] Séjean, M. and Binctin, N. (2019) Sûretés Réelles Mobilières sur la Propriété Intellectuelle. *Revue Internationale de Droit Comparé*, 71 (2).

[58] UNCITRAL (2011) UNCITRAL *Legislative Guide on Secured Transactions. Supplement on Security Rights in Intellectual Property*. Rome. Available from: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/10-57126_ebook_suppl_sr_ip.pdf [Accessed 28 June 2025].

[59] UNIDROIT (2023) UNIDROIT *Principles on Digital Assets and Private Law*. Rome. Available from: https://www.unidroit.org/wp-content/uploads/2024/01/Principles-on-Digital-Assets-and-Private-Law-linked-1.pdf [Accessed 28 December 2024].

[60] Weber, R.H. (2017) Improvement of Data Economy through Compulsory Licenses? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[61] Wiebe, A. (2016) Protection of industrial data – a new property right for the digital economy? *GRUR International – Journal of European and International IP Law*, (10).

[62] Wiebe, A. (2023) The Data Act Proposal. Access rights at the Intersection with Database Rights and Trade Secret Protection. *Gewerblicher Rechtsschutz und Urheberrecht*, (4).

[63] World Intellectual Property Organization (2002) *Summary on Existing Legislation Concerning Intellectual Property in Non-Original Databases*. SCCR/8/3. Geneva. Available from: https://www.wipo.int/edocs/mdocs/copyright/en/sccr_8/sccr_8_3.pdf [Accessed 24 June 2025].

[64] van Erp, S. (2017) Ownership of Data: The Numerus Clausus of Legal Objects. *Brigham-Kanner Property Rights Conference Journal*, (6).

[65] Verhagen, H.L.E. (2022) *Security and Credit in Roman Law*. Oxford: Oxford University Press.

[66] Vivant, M. (2006) La Privatisation de l'Information par la Propriété Intellectuelle. *Revue Internationale de Droit Économique*, vol. XX (4).

[67] *Your Response Ltd v. Datateam Business Media Ltd* (2014) Court of Appeal, 3 WLR, p. 887.

[68] Zech, H. (2012) *Information als Schutzgegenstand*. Tübingen: Mohr Siebeck.

[69] Zech, H. (2015) Information as Property. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, 6 (3).

[70] Zech, H. (2015) „Industrie 4.0“ – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt. *Gewerblicher Rechtsschutz und Urheberrecht*, (12).

[71] Zech, H. (2016) A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice*, 11 (6).

[72] Zech, H. (2016) Data as a Tradeable Commodity. In: Alberto De Franceschi (ed.) *European Contract Law and the Digital Single Market*. Cambridge–Antwerp–Portland: Intersentia.

[73] Zimmer, D. (2017) Property Rights Regarding Data? In: Sebastian Lohsse, Reiner Schulze, Dirk Staudenmayer (eds.) *Trading Data in the Digital Economy: Legal Concepts and Tools*. Baden-Baden: Nomos–Hart.

[74] Żok, K. (2020) Zastaw Antychretyczny – Zagadnienia Konstrukcyjne. In: Karol Szadkowski, Krzysztof Żok (eds.) *Zabezpieczenia Wierzytelności*. Warszawa: Wolters Kluwer.