III. Personal Data Meets Sui Generis Database Right

As discussed, the RtDP is not an absolute right, since it shall not adversely affect rights and freedoms of others. In view of its broad wording, and considering the RtDP's legislative history and purpose, there are sound reasons to interpret 'rights of others' as encompassing IPRs.

Among the IPR candidates is the SGDR under the DbD. Interesting enough, during discussions of the GDPR's proposal in the Council, the French delegation already raised the potential clash between the RtDP and the SGDR.[141] Hence, the conflict might not have been as silent as suggested.[142]

A. The EU Database Directive

Legal protection under the DbD is afforded to databases in any form, while computer programs used in relation thereto are expressly excluded.[143] The DbD's wording is quite broad and technically neutral.[144] Reference to 'any form' comprises all types of databases, regardless of format – electronic and non-electronic databases are covered.[145] The legislator's aim was to provide for 'a wide scope, unencumbered by considerations of a formal, technical or material nature'.[146]

Besides harmonization of national laws in relation to copyright protection of original databases,[147] the DbD also intended to incentivize investment in the production of databases in the EU through the introduction of a new sui generis right – the SGDR.[148] Such right provides database pro-

141 Council Doc ST 9897 2012 REV 1 (14.05.2012) 55.
142 Graef, Husovec and Purtova (n 7) 10.
143 DbD art 1(1), (3).
144 DG CONNECT, 'Study in Support of the Evaluation of Directive 96/9/EC on the Legal Protection of Databases – Final Report' (prepared for the Commission by JIIP, Technopolis, and Individual Experts Lionel Bently and Estelle Derclaye) [2018] SMART 2017/0084 (Second Evaluation Report) 4.
145 DbD rec 14.
146 Case C-444/02 *Fixtures Marketing v OPAP* [2004] ECLI:EU:C:2004:697 para 20.
147 DbD rec 2.
148 DbD rec 12.

ducers with an additional layer of protection, resulting in a two-tier protection regime.[149]

The introduction of a novel IPR was justified by the legislator on the significant disparity in the level of investment and legal protection of databases within the EU, but most importantly if compared to the US.[150] It was assumed that the rise of a market for modern information storage and processing systems would require protection against misappropriation to reach its full value.[151]

1. Defining a Database

To be classified as a 'database' under Article 1(2) DbD three cumulative criteria have to be fulfilled: (i) it must consist of a 'collection of independent' elements (ie works, data or other materials); (ii) such elements have to be 'arranged in a systematic or methodical way' and (ii) they must be 'individually accessible'.

The first criterion is that the compilation is a collection of independent elements. There is no minimum number of combined elements to find a database.[152] Although the term 'collection' might resemble a static notion, there is no restriction for the protection of dynamic databases (actually, the protection requirement of 'verification' sustains it, as discussed below).

The fact that the elements have to be independent is of greater relevance.[153] Elements composing audio-visual, cinematographic, literary, or musical works are not considered independent.[154] In the absence of such requirement, there would be a risk of complete overlap with copyright and neighbouring rights.[155] Not only individual pieces of information can con-

149 Commission, 'DG Internal Market and Services Working Paper: First Evaluation of Directive 96/9/EC on the Legal Protection of Databases' [2005] <http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf> accessed 7 April 2018 (First Evaluation Report) 6.

150 DbD rec 11.

151 DbD recs 12, 39.

152 *Fixtures Marketing* (n 146) para 24.

153 Matthias Leistner, *Der Rechtsschutz von Datenbanken im deutschen und europäischen Recht: eine Untersuchung zur Richtlinie 96/9/EG und zur Umsetzung in das deutsche Urheberrechtsgesetz* (Beck 2000) 372, 46.

154 DbD rec 17.

155 P Bernd Hugenholtz, 'Something Completely Different: Europe's Sui Generis Database Right' in Frankel S and Gervais D (eds), *The Internet and the Emerging*

stitute an independent element, but also a combination of pieces fulfils the requirement.[156]

Furthermore, the CJEU held that independency means an autonomous informative value of the elements, ie when separated from the collection, their contents' value must not be affected.[157] More recently, the Court gave an extensive interpretation thereto by ruling that the value has to be considered from the perspective of the person interested in the separate element.[158] It will be independent if the element is used for financial gain and in an autonomous manner, and provides the person using it with relevant information.

The second criterion is that the elements must be arranged in a systematic or methodical way, but 'it is not necessary for those materials to have been *physically* stored in an organized manner'.[159] It is directly connected to the third criterion of individual accessibility. As long as there is a technical or other means (eg an index, or a particular plan or method of classification) enabling their retrieval from an unorganized collection, the requirements are met.[160]

The result is an overly broad and open-ended definition hardly ever excluding protection.[161] More or less any set of elements can constitute a database under the DbD. For instance, the CJEU has dealt with cases involving databases composed by sports data, legal databases, lists of poems, lists of automobiles, websites selling air travel service and maps.[162]

Importance of New Forms of Intellectual Property (Information Law Series v 37, Kluwer Law International 2016) 205, 211.

156 Case C-490/14 *Verlag Esterbauer* [2015] ECLI:EU:C:2015:735 para 20.

157 *Fixtures Marketing* (n 146) paras 32-3.

158 *Verlag Esterbauer* (n 156) para 37.

159 DbD rec 21 (emphasis added).

160 *Fixtures Marketing* (n 146) para 30.

161 P Bernt Hugenholtz, 'Data Property in the System of Intellectual Property Law: Welcome Guest or Misfit?' in Lohsse S, Schulze R and Staudenmayer D (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools Münster Colloquia on EU Law and the Digital Economy III* (Nomos 2017) 75, 88.

162 Second Evaluation Report (n 144) 5.

2. The Sui Generis Database Right

(a) Protection Requirement

Precondition for protection under the SGDR is the quantitative and/or qualitative substantial investment in either obtaining, verifying or presenting the contents of a database.[163]

(1) The Substantial Investment Requirement

The investment has to be substantial from a quantitative and qualitative perspective. Not only monetary resources deployed by the database maker must be considered, but also human and technical efforts.[164] The quantitative assessment refers to quantifiable resources, such as money and time, and the qualitative assessment to efforts, which cannot be quantified, such as intellectual effort or energy. This means that databases, which do not require high monetary investments, are also protectable, as long as there is a substantial investment of time or effort.

There is no established threshold for the quantum of 'substantial investment' required.[165] Although national courts had different approaches, a relatively low-level of investment sufficed.[166] For instance, the *Bundesgerichtshof* (BGH – German Federal Supreme Court) held that the requirement would be fulfilled if, objectively speaking, no completely insignificant expenses were necessary to create the database.[167]

Even though the absence of a threshold might lead to some uncertainties, a minimum quantum could be discriminatory, excluding small

163 DbD art 7(1).

164 *Fixtures Marketing* (n 146) para 44.

165 Annemarie C Beunen, *Protection for databases: the European Database Directive and its effects in the Netherlands, France and the United Kingdom* (Wolf Legal 2007), 138; Mark J Davison and P Bernt Hugenholtz, 'Football Fixtures, Horseraces and Spin-Offs: the ECJ Domesticates the Database Right' (2005) 27 (3) EIPR 113, 116; Estelle Derclaye, *The legal protection of databases: a comparative analysis* (Edward Elgar 2008) 362, 75; Second Evaluation Report (n 144) 7.

166 Second Evaluation Report (n 144) 7-8.

167 BGH, GRUR 2011, 724 – Case I ZR 196/08 – *Zweite Zahnarztmeinung II* para 23, 'Es reicht aus, wenn bei objektiver Betrachtung keine ganz unbedeutenden, von jedermann leicht zu erbringenden Aufwendungen erforderlich waren, um die Datenbank zu erstellen. Nicht notwendig sind Investitionen von substanziellem Gewicht'.

database makers from protection.[168] The flexible criterion allows for an assessment on an individual basis, including future impact of technological developments.[169]

(2) Investment in Obtaining, Verifying or Presenting

Not any investment counts towards the protection requirement under the SGDR – only substantial investment in (i) obtaining, (ii) verifying or (iii) presenting the contents of a database is relevant. The acts are non-cumulative, which means that either one renders the investment eligible for protection.[170]

The most disputed term was 'obtaining', as it can be construed narrowly or broadly.[171] In *BHB* and *Fixtures Marketing*, the CJEU adopted the former, by distinguishing between creation and collection of the elements.[172] Based on the SGDR's purpose to promote and protect investment, the relevant investment must refer to the creation of the database as such.[173] Consequently, it refers to 'resources used to seek out existing independent materials and collect them in the database, and not to the resources used for the creation as such of independent materials'.[174]

The decision was very welcomed, as it provided a solution (even if partial) for the issue of monopolistic sole-source databases.[175] This was the case in both judgments, where the data composing the databases (list of horseraces and football fixtures, respectively) could not be collected independently, as they were forged by the database makers themselves. As the databases were generated as a by-product of another main activity (ie the organization of horse races and football matches), no substantial investment was actually made on the collection of existing elements, but in their creation. By distinguishing between obtaining and creating, protection for

168 Beunen (n 165) 140; Derclaye (n 165) 91.
169 Beunen (n 165) 141.
170 Ibid 107; Derclaye (n 165) 92.
171 Derclaye (n 165) 92.
172 Case C-203/02 *British Horseracing Board* [2004] ECLI:EU:C:2004:695 (BHB) para 31; *Fixtures Marketing* (n 146) para 40.
173 *BHB* (n 172) para 30.
174 Ibid 31; *Fixtures Marketing* (n 146) para 40.
175 Davison and Hugenholtz (n 165) 114; Derclaye (n 165) 94; Matthias Leistner, 'The Protection of Databases' in Derclaye E (ed) *Research Handbook on the Future of EU Copyright* (Edward Elgar 2009) 427, 437.

sole-source databases was denied, where no substantial investment in obtaining, verification or presentation of the elements created could be evidenced.[176]

Nevertheless, the distinction is not always straightforward.[177] It has been questioned whether data from natural phenomena, stock market rates, or machine-generated data should be categorized as obtaining or creating.[178] Leistner's teleological interpretation provides for some light.[179] Considering that the cases appreciated by the CJEU involved data that were created in the sense of 'made-up' or 'invented', protection would be available only to such pre-existing data that is capable of being independently collected, measured or observed by a third party.

Although the CJEU did not yet decide on a case in this regard,[180] the BGH adopted this approach in the *Autobahnmaut* case.[181] Data collected by a toll company using its tolling system regarding fuel card numbers, vehicle registration numbers, date of the toll journeys and the length of the routes travelled, was considered obtained data.[182] Under BGH's reasoning, such data could be independently collected by a third party, not having been created by the company.

Regarding the act of 'verifying', the CJEU held that it refers to ensuring the reliability of information within the database, as well as monitoring accuracy of the elements collected when of the database's creation or operation.[183] It includes acts of checking, correcting and updating the database's contents,[184] which are of special relevance in case of dynamic databases.[185]

---

176 *BHB* (n 172) para 35.
177 Beunen (n 165) 126; Davison and Hugenholtz (n 165) 115; Hugenholtz, 'Data Property' (n 161) 87; Leistner, 'Protection of Databases' (n 175) 437.
178 Beunen (n 165) 126; Davison and Hugenholtz (n 165) 115; Hugenholtz, 'Data Property' (n 161) 87.
179 Leistner, 'Protection of Databases' (n 175) 438.
180 Matthias Leistner, 'Big Data in the Digital Economy: Legal Concepts and Tools' in Lohsse S, Schulze R and Staudenmayer D (eds), *Trading Data in the Digital Economy: Legal Concepts and Tools Münster Colloquia on EU Law and the Digital Economy III* (Nomos 2017) 27, 28-9, also considers the CJEU's decision in *Verlag Esterbauer* as supporting the distinction.
181 BGH, GRUR 2010, 1004 – Case I ZR 47/08 – *Autobahnmaut*.
182 Ibid para 19.
183 *Fixtures Marketing* (n 146) para 43.
184 Hugenholtz, 'Something Completely Different' (n 155) 212.
185 Beunen (n 165) 134.

Any verification conducted during creation of the elements themselves is ruled out.[186]

Finally, the CJEU found that investment in 'presenting' refers to resources used to give the database its processing information function, 'that is to say those used for the systematic or methodical arrangement of the materials (…) and the organisation of their individual accessibility'.[187] Acts of digitalization of analogue files, creation of a table of contents or thesaurus, or design of user interfaces are within the concept.[188]

(b) Ownership – the Database Maker

According to Article 7(1) DbD, the SGDR is vested in the database maker, ie 'the person who takes the initiative and the risk of investing' (excluding subcontractors).[189] It encompasses natural and legal persons and is consistent with the right's objective to protect investment.[190] This broad definition can lead, however, to significant problems and uncertainties.[191]

Although the DbD does not provide for joint ownership (nor regulates it) the vague criteria to determine the right holder easily leads to such scenario.[192] Whenever two or more persons take the initiative and risk of investment in the creation of a particular database, there will be joint ownership. Especially in cooperative and open innovation networks, as well as in data sharing platforms for connected devices, there is a high probability of co-ownership.[193]

Contractual provisions could regulate it, but it is not uncommon that the parties do not even realize that the resulting database will be jointly owned.[194] Without such awareness, no appropriate provision is included in agreements. Moreover, there might be different bargaining powers, especially in consumer relations.[195] Even if contractually regulated, the outcome might not be the most desired one from a policy perspective.

---

186 *BHB* (n 172) para 34; *Fixtures Marketing* (n 146) para 50.
187 *Fixtures Marketing* (n 146) para 43.
188 Hugenholtz, 'Something Completely Different' (n 155) 211.
189 DbD rec 41.
190 Leistner, 'Big Data' (n 180) 35.
191 Ibid 35.
192 Second Evaluation Report (n 144) 31.
193 Ibid 31-2; Drexl, 'BEUC Study' (n 43) 77; Leistner, 'Big Data' (n 180) 35.
194 Leistner, 'Big Data' (n 180) 35-6.
195 Ibid.

If the persons creating the database might already have issues in determining who is/are its owner(s), it is even more difficult and burdensome for third parties to precisely know who the database maker is.

(c) Scope of Protection

The SGDR provides an exclusive right to prevent (i) extraction, and (ii) reutilization, 'of the whole or of a substantial part, evaluated qualitatively and/or quantitatively, of the contents of that database'.[196] As a rule, the right lasts for 15 years following the date of completion of the database.[197]

The act of extraction is defined as 'the permanent or temporary transfer of all or a substantial part of the contents of a database to another medium by any means or in any form'.[198] As the SGDR does not confer an exclusive right over information per se,[199] there is no protection against independently created databases where the elements are obtained from other sources than the relevant database.[200] This, however, does not exclude the possibility of an indirect infringement, neither a *de facto* control over the data by the database maker (as discussed below).

No technical reproduction is needed to find an infringing extraction, as the CJEU interpreted the term extensively. It includes 'any unauthorised act of appropriation of the whole or a part of the contents of a database'.[201] It is sufficient that the elements were consulted and copied (even by hand) from the concerned database.[202] Accordingly, good documentation of the creation process is recommended.

The act of reutilisation is specified as 'any form of making available to the public all or a substantial part of the contents of a database, by renting, by on-line or other forms of transmission'.[203] In *BHB*, the CJEU gave the

196 DbD art 7(1).
197 DbD arts 10(1)-(2). In case of substantial change, evaluated qualitatively or quantitatively, to the contents of a database, which results in the database being considered a substantial new investment (also evaluated qualitatively or quantitatively), qualifies the database resulting from that investment for its own term of protection (art 10(3) DbD).
198 DbD art 7(2)(a).
199 Leistner, *Rechtsschutz* (n 153) 146-47.
200 Derclaye (n 165) 107; Leistner, 'Protection of Databases' (n 175) 431.
201 Case C-304/07 *Directmedia Publishing* [2008] ECLI:EU:C:2008:552 para 34.
202 Hugenholtz, 'Something Completely Different' (n 155) 213.
203 DbD art 7(2)(b).

term a broad interpretation, holding that it refers 'to any act of appropriating and making available to the public, without the consent of the maker of the database'.[204]

The provision does not consider the intent or purpose of the acts of extraction or reutilization, providing for an objective infringement test.[205] It is irrelevant, for instance, if the contents of a database are extracted or reutilized to create a competing database or for any other purpose whatsoever.[206]

In the absence of an extraction or reutilization of the database's entire content, the unlawful acts are limited to substantial parts. The intrinsic economic value of the element affected is irrelevant to assess the substantial part.[207] Rather, the substantial investment made by the database maker in obtaining, verifying or presenting the content, as well as the detriment to the data maker's investment should be considered.[208]

In quantitative terms, the substantial part refers to the volume of elements extracted or reutilized from the database in relation to the volume of the database's contents as a whole.[209] The comparison must be with the database subject to extraction or reutilization. For infringement assessment, it is immaterial whether such part subsequently is considered substantial in relation to another database where it is incorporated.[210] The volume threshold has to be established on a case-by-case basis.[211]

A qualitatively substantial part 'refers to the scale of the investment in the obtaining, verification or presentation of the contents of the subject of the act of extraction and/or reutilisation, regardless of whether that subject represents a quantitatively substantial part'.[212] The elements extracted or reutilized have to reflect the money, time and/or effort invested by the database maker. Even a quantitatively small part can represent significant human technical or financial investment.[213] The CJEU thus clearly corre-

204 *BHB* (n 172) para 51.
205 Derclaye (n 165) 119.
206 *BHB* (n 172) para 47.
207 Ibid 72.
208 Ibid 69.
209 Ibid 70.
210 Beunen (n 165) 186; Derclaye (n 165) 110.
211 Derclaye (n 165) 113.
212 *BHB* (n 172) para 71.
213 Ibid 71.

lates the 'substantial investment' requirement for protection and the 'substantial part' requirement for infringement.[214]

In order to prevent the provision's circumvention, Article 7(5) DbD determines that repeated and systematic extraction and/or reutilization of insubstantial parts are unlawful if they (i) conflict with a normal exploitation of the database, or (ii) unreasonably prejudice the legitimate interests of the database maker. The provision intents to avoid extraction of insubstantial parts, which add up and effectively result in the 'reconstitution of the database as a whole or, at the very least, of a substantial part of it'.[215] It is therefore necessary that each insubstantial part differs from each other to jointly make up a substantial part.[216]

In *BHB*, the SGDR's scope was further broadened, as the CJEU ruled that indirect extraction and reutilization are covered.[217] Accordingly, extraction and reutilization based on a third party's copy of the database are equally infringing.[218] The Court's reasoning relies on Article 7(2)(b) DbD, which sets forth that exhaustion after the first sale of a copy only applies to the right to resell that copy.

(d) Exceptions and Limitations

In line with the SGDR's scope, Article 8(1) DbD determines that lawful users might extract and reutilize insubstantial parts of the contents of a database, evaluated qualitatively and/or quantitatively, for any purposes whatsoever. The assessment of an 'insubstantial part' essentially follows the negative of the 'substantial part' test. The provision is binding, whereby any contractual provision to the contrary is deemed null and void.[219] Although not included under the exceptions title of Article 9 DbD, the provision can be considered one.[220]

Article 9 DbD lists exhaustively three optional exceptions, which can be implemented under national legislation: (i) private purposes regarding

214 Derclaye (n 165) 111; Davison and Hugenholtz (n 165) 116.
215 *BHB* (n 172) para 87.
216 Leistner, *Rechtsschutz* (n 153) 181.
217 *BHB* (n 172) paras 52-3.
218 Davison and Hugenholtz (n 165) 117.
219 DbD art 15. The CJEU held in *Ryanair* that the lawful user's right is not guaranteed in case of databases not protected under the DbD. Case C-30/14 *Ryanair* [2015] ECLI:EU:C:2015:10.
220 Beunen (n 165) 212.

non-electronic database; (ii) illustration for non-commercial teaching or scientific research; and (iii) public security or an administrative or judicial procedure. While the first two only cover extraction, the latter refers to both extraction and reutilization. Furthermore, the exceptions only cover extraction and/or reutilization of substantial parts (not the whole) of the contents of the database, which are made available to the public by the database maker.

The provision has been very criticized in the literature, as well as in the framework of the evaluations on the DbD.[221] *First*, the DbD does not provide for mandatory exceptions and limitations for the SGDR, which leads to problems in terms of harmonization. *Second*, especially if compared to copyright provisions, the list of exceptions is very limited in scope. In addition, the initially proposed compulsory licensing provision was left out from the DbD's final version.

B. Intersection between the Right to Data Portability and the Sui Generis Database Right

After delineating and analysing the RtDP and the SGDR, this chapter now turns to their intersection. Two specific scenarios are discussed; namely, online platforms and connected devices – the first one given the legislator's focus on them when proposing and discussing the RtDP; the second, in view of its growing importance in individual's daily activities.

1. Personal Data as Contents of a Database

As discussed, a database is defined as a collection of independent elements, where they must be systematically or methodically arranged, and individually accessible. The concept of 'independent elements' is quite broad and includes works, data or any other materials. A broad concept also holds true for 'personal data', as any information that may lead to the data subject's identification is covered. Considering that identifiability is highly po-

221 Ibid 212, 228-9; Drexl, 'BEUC Study' (n 43) 81; Annette Kur and others, 'First Evaluation of Directive 96/9/EC on the Legal Protection of Databases - Comment by the Max Planck Institute for Intellectual Property, Competition and Tax Law, Munich' (2006) 37 IIC 551, 556-7; Leistner, 'Big Data' (n 180) 47; First Evaluation Report (n 149) 21-2; Second Evaluation Report (n 144) 15-6.

tentialized by current technologies, a clear distinction between personal and non-personal data seems to be evanescing.

Each piece of personal data is separable from one another and carries an autonomous informative value. Names, addresses, e-mails, location data, and photos are all concomitantly personal data and independent elements that convey a relevant information. In a big data scenario, even the most trivial piece of data might be useful,[222] as well as the combination of two of them.[223] It is, therefore, quite straightforward that personal data is able to form a collection of independent materials.

However, to be classified as a database, personal data still has to be arranged systematically or methodically, and be individually accessible. For instance, telephone directories, lists of e-mail addresses, addresses for mobile phones, names and associated data of persons working at doctor practices, motorway toll databank, and customer lists have already been considered databases under national laws.[224]

The question is, therefore, when personal data provided by the data subject (as per the RtDP) is systematically or methodically arranged, and individually accessible.

(a) Online Platforms

Online platforms contain vast amounts of personal data, which are either active and knowingly provided by the user (such as name, e-mail, age, photos and comments), or collected through observation (such as browsing history, user and purchase preferences, and location data). In view of the identifiability criterion, the majority of the contents created and posted by users will fall under the concept of personal data.[225]

Personal data is usually arranged within online platforms in such a way that it can be individually retrieved. All pieces of information are classified and organized based on certain criteria.[226] Take Facebook, for example, where you have different tabs in the user's profile for each information (timeline, about, friends, photos, etc). Some information is even concomi-

222 Herbert Zech, 'A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data' (2016) 11 (6) JIPLP 460, 467.
223 Drexl, 'BEUC Study' (n 43) 75.
224 Second Evaluation Report (n 144) 5-6, 92, fn 149.
225 Metzger and others (n 135) 103.
226 Graef, *Essential Facility* (n 6) 142.

tantly arranged under multiple categories, such as photos, which are in the timeline, or organized according to its source and date within the 'photo' tab. Electronic retrieval functions are even enhanced through internal search and filter functions.

Consequently, it is possible for online platforms whose content is composed by personal data to be classified as a database under the DbD.[227] Furthermore, each individual user profile/account, as well as the entire online platform can be qualified as a database. In the former case, there is a collection of data on a specific data subject, while in the latter, the collection includes data on several individuals.

(b) Connected Devices

All kinds of daily 'things' are becoming connected to the Internet – from the toothbrush to the coffee machine, going through the front door lock, and entering the car. Although the type of data collected by each connected device is dependent on its function,[228] they for certain increasingly are able to collect personal data through observation, such as location, heartbeats, and temperature.[229]

Data collected by such devices comes from different sources – from integrated sensors, as well as from wireless communication.[230] In addition, their use is usually linked to some service provision or online platform, where individuals provide additional personal data.

All data obtained (as per the DbD) by connected devices, including personal data, will most frequently be structured in databases.[231] The probability of data being collected and not structurally arranged is very remote, as it would render the collection useless.[232] Different pieces of raw data are combined (for example, with additional date, time and location data) to arrange them systematically,[233] and enable its individual retrieval. Conse-

227 Ibid.
228 Drexl, 'BEUC Study' (n 43) 41.
229 As discussed (see II.B), when the Commission referred to home temperature sensors, it recognized that data collected through connected devices might refer to personal and non-personal data. COM(2017) 9 final (n 2) 9.
230 Drexl, 'BEUC Study' (n 43) 41; Second Evaluation Report (n 144) 29.
231 Zech (n 222) 468.
232 Ibid.
233 Drexl, 'BEUC Study' (n 43) 74.

quently, collections of data from connected devices can generally constitute a database under the DbD.[234]

2. Controllers as Database Makers Making a Substantial Investment

For the above databases to qualify for protection under the SGDR, the controller still must qualify as a database maker and there has to be a substantial investment in obtaining, verifying or presenting their contents.

(a) Online Platforms

The operator of an online platform is undoubtedly a controller under the GDPR, as this person, alone or jointly with others, determine the purposes and means of the processing of personal data. There is also little doubt that significant resources are required to set up such platforms to collect personal data from individuals and keep them updated.[235]

The initiative and risk of investment will frequently be taken by the online platform operator. In terms of 'obtaining', the investment in software development does not count, but all effort to make the platform attractive to users and convincing them to use it and provide personal data certainly do.

Under the CJEU's obtaining-creating differentiation, however, a potential issue could arise from content posted by users, which is not pre-existing (such as a photo taken within the social network using the smartphone's camera, filming a live story, or a text spontaneously written by the user).[236] Thus, one could argue that the data is being created, not obtained. However, it is necessary to distinguish between elements created by the database maker itself and by third parties. Taking into consideration the teleological interpretation, it is clear that the data could be independently obtained by third parties, as they are usually not owned or made-up by the

234 Ibid 66-7; Hugenholtz, 'Data Property' (n 161) 88; Zech (n 222) 467.

235 Graef, *Essential Facility* (n 6) 481.

236 Graef, *Essential Facility* (n 6) 142-3 also argues that from the obtaining-creating distinction, online platforms could have an issue in claiming Database Right on data that is inferred from the user's use of the platform. However, considering that inferred data is generally not considered data 'provided by the data subject' under the RtDP, it is not of an issue for the specific analysis of this research.

online platform.[237] Another possibility is to consider such live-created contents as composed by two stages – in a first step, the user creates the content (ie takes the photo, films the video or writes the text), on a second, she posts and the database maker obtains it. Therefore, there seems to be no reason to exclude live created contents from the DbD's concept of obtaining.

A substantial investment in verifying the contents is also present, as online platforms constantly gather, check and update user data.[238] Old data is not enough to keep most online platforms attractive, as some data may lose its veracity, such as contact details and preferences.[239] See for instance the messages from Facebook reminding users to update their contact details or to link their account to their mobile numbers, or the e-mails from Instagram and Pinterest showing recent posts and inviting the user to access the platform.

Finally, the effort to make the platform attractive to users is directly tied with the investment in presenting database's contents. The design of a user-friendly interface is key for online platforms, which leads to constant investment for improvements.

Considering the above, it is possible for online platforms to rely on the SGDR whenever there is evidence of a substantial investment in obtaining, verifying and presenting the data.[240]

(b) Connected Devices

The controller in case of a connected device might be its manufacturer and/or any third-party providing services there through, depending on who decides how and why personal data is processed. With regard to the database maker, the situation is far from clear.

There is currently no unanimity whether databases originating from connected devices are protectable under the SGDR.[241] While Drexl and Leistner understand that the SGDR's low threshold may easily lead to pro-

237 Some of the major online platforms and social networks (such as Facebook, Instagram, Snapchat, TripAdvisor, Twitter and YouTube) recognise under their Terms of Use/Service the user's ownership and/or copyright on the content she posts.
238 Graef, *Essential Facility* (n 6) 488.
239 Ibid 504.
240 Ibid 143.
241 Second Evaluation Report (n 144) 30.

tection,[242] the Second Evaluation Report on the DbD concludes that it likely does not, as the databases' generation is closely related to data creation.[243]

From the Report's statement, the main issue for recognizing the SGDR is the obtaining-creating rule.[244] However, as discussed, data collected through observation by connected devices could fall within 'obtaining' under the teleological interpretation. The data is not made-up by the database maker and could (at least in theory) be independently obtained by others. This also seems to be the BGH's approach in *Autobahnmaut*.[245]

Although investment in developing connected devices or software does not amount towards the obtaining requirement,[246] setting up infrastructure for measuring, obtaining or documenting might.[247] The constant collection and updating of the database's contents fulfils the verification requirement. In addition, structuring the data methodically or systematically also counts for the presentation requirement.[248] Therefore, databases from connected devices might also frequently rely on the SGDR.[249]

The question in whom the SGDR will be vested is less clear. It could be argued that the individual acquiring or using the device also makes an investment and takes the risk to have her data collected.[250] However, considering the 'initiative' requirement, it will usually be vested in the connected device's manufacturer.[251] Consequently, the manufacturer might concomitantly be the controller and the database maker.

3. The Sui Generis Database Right as 'Rights of Others'

As discussed, there are no sound reasons to interpret 'rights of others' under the RtDP as excluding IPRs. Notwithstanding its sui generis character

242 Drexl, 'BEUC Study' (n 43) 68; Leistner, 'Big Data' (n 180) 27-8.
243 Second Evaluation Report (n 144) Executive Summary, ii.
244 Drexl, 'BEUC Study' (n 43) 70.
245 *Autobahnmaut* (n 181).
246 Ibid 63.
247 Leistner, 'Big Data' (n 180) 29, 37.
248 Ibid 29.
249 Drexl, 'BEUC Study' (n 43) 85; Same understanding of the majority of experts consulted for the Second Evaluation Report (n 144) 131.
250 Second Evaluation Report (n 144) 32.
251 Drexl, 'BEUC Study' (n 43) 77; Leistner, 'Big Data' (n 180) 37; Second Evaluation Report (n 144) 32.

and the peculiarities surrounding its protection requirements, the SGDR can be considered a type of IPR.[252] Thus, it could be invoked by controllers to refuse a portability request.[253]

Although the preferred approach is that 'others' does not include the controller, considering the unclear wording, one cannot disregard the risk of courts interpreting the provision otherwise. Moreover, even in cases where the recommended interpretation is adopted, the SGDR could still be claimed in the event of joint ownership, which might be more common than expected.

4. Data Portability Request as Extraction or Reutilization of the Contents of a Database

The remaining question is if a portability request can adversely affect the database maker's SGDR. A potentially adverse effect on the SGDR could arise from an unlawful act affecting the right's investment protection function, ie one that is not permitted under its scope, nor excused by an exception.

The Commission, when referring to the absence of a RtDP in 2012, stated that 'there is also no explicit right for the individual to *extract* his/her own personal data (…) from an application or service'.[254] This indicates that the RtDP possibly comes very close to the database maker's right to prevent extraction of the contents of its database.

In view of *BHB*'s ruling that the SGDR's scope covers indirect extraction or reutilization, both the data subject, as well as the receiving controller might commit an infringing act. The likelihood of the latter would be higher where the receiving controller offered the data subject some kind of incentive to exercise her RtDP.[255] The experience with the telecom number portability showed that suppliers might very well be willing to give discounts, extra credits or the alike to convince someone to port.

As the individual's personal data composes the database's contents, the exercise of the right to both direct and indirect portability will result in a permanent transfer of the personal data content to another medium. Whether the extraction amounts to a substantial or insubstantial part, will

252 Beunen (n 165) 14.
253 Drexl, 'BEUC Study' (n 43) 83-4.
254 SEC(2012) 72 final (n 20) 28 (emphasis added).
255 Graef, Husovec and Purtova (n 7) 16.

essentially depend on the definition of the database from where content is retrieved.

In view of this, a database maker could attempt to influence the assessment's outcome by narrowing the database's size.[256] Rather than considering the entire universe of online platform or connected devices users, the database maker could limit the database to the contents relating to the specific individual requesting portability. While in the first case, the volume extracted could be considered insubstantial in comparison to the whole, in the second it would likely be substantial. Consequently, a portability request could potentially be understood as an unlawful extraction.

The database maker's right to prevent the reutilization of substantial parts of its database's contents might also be infringed. The data subject or the receiving controller could make the content available to the public by online transmission, for example.[257] Whenever the concerned personal data is made available to an indeterminate number of persons (such as on an online platform), a 'making available to the public' could be found and, thus, an infringing act.

Even in case of an extraction or reutilization of insubstantial parts there might still be an infringement if the acts are repeated and systematic. A possible interpretation would consist of reiterated portability requests from one data subject to the same controller.[258] However, it seems unlikely that such reiterated requests from one individual would include insubstantial parts if compared to a database concerning her, or that the substantial parts would amount to a substantial part in relation to the whole database.

A possible extensive interpretation would consist of portability requests from different data subjects to the same controller, whereby such individuals received an incentive from a third party to make the request. In this case, the sum of the personal data contents of different individuals could represent a substantial part of the whole database and an indirect act of extraction by the receiving controller.

256 Beunen (n 165) 189-90.

257 Graef, Husovec and Purtova (n 7) 15.

258 Although reiterated portability requests are not prohibited under the GDPR, Article 12(5) GDPR determines that excessive portability requests, in particular because of their repetitive character, allow the controller to charge a reasonable fee or even refuse the request. The GDPR does not determine what would be considered 'repetitive', or in which cases the controller would actually be able to refuse the portability instead of only charging a fee.

The above acts could still not infringe if one of the exceptions from the SGDR comes into play,[259] but none seems applicable to the RtDP. The only potential candidate is the extraction for personal use in case of an indirect portability, where the data subject, after receiving her personal data from the original controller, decides not to forward it to a new controller, but keep it for herself on a private device. However, this hypothesis is very limited and does not meet the RtDP's rationale.

The above analysis shows that there is indeed a possible clash between the RtDP and the SGDR, whereby the second could be invoked to bar the first.[260]

259 As the exceptions are not mandatory, applicability would further depend whether and to what extend they were implemented under national laws.

260 Drexl, 'BEUC Study' (n 43) 83-4.