ii) Requirements for Protection

To the extent that ownership could indeed be applied to unstructured data no specific requirements apply.

iii) Owner

Both single and joint ownership are possible and both a natural or a legal person can be(come) the owner.

Some legal scholars have the opinion that the rule according to which public possession of corporeal, movable goods constitutes a presumption of ownership (Article 2279 CivC and Article 3.28 new CivC) could also – at least in theory – apply to incorporeal, movable goods, and thus to unstructured data (i.e. that the one who possesses such data can be presumed to be the owner).[16] On the other hand, others argue that de facto control of data does not necessarily amount to ownership since unstructured data could be in the possession of various parties. The latter is even more true for personal data – although it is not the subject of this contribution – since the data subjects have rights to protect their data (e.g. to have such data deleted). Therefore, data controllers do not have ownership rights in such data but only rights to control the use of such data.

iv) Scope of Protection

Ownership is the most comprehensive and exclusive property right and is a so-called *perpetual right*. It grants the owner exclusively all powers in the property, except for those transferred to third parties or prohibited by law. Restrictions could be, for instance, IP rights that grant a sometimes similar yet also different protection than ownership rights (*see* 2.3.4).

The scope of protection of property rights and IP rights, although interconnected, have remarkable differences. Therefore, it is not always clear how these relate to each other.[17]

As stated above, classical criminal concepts have been applied to ICT data in the past (such as theft, breach of trust, concealment, fraud and embezzlement) in order to protect the economic value of the data and therefore the owner's patrimony. It seems that the scope of protection of property rights that initially concerned the data's medium was then extended to the original data, and eventually to all copies made of the original data. It is at this stage unclear whether this means that unstructured data can be the object of property rights or if only defensive rights are granted against the unlawful acquisition of data, without rights in rem in unstructured data. To the

16. Wian Erlank, 'Books, Apps, Movies and Music – Ownership of Virtual Property in the Digital Library', 207 *EPLJ* (2013) p. 2; Matthias E. Storme, 'De Drievoudige Gelaagdheid van Schuldvorderingen en hun Bescherming', in *Liber Amicorum W. Van Gerven* (Kluwer, 2000) pp. 331-332; René Dekkers & Eric Dirix, *Handboek Burgerlijk Recht, II, Zakenrecht. Zekerheden. Verjaring.* (Intersentia, 2005) p. 537.
17. For a thorough analysis, *see* Bernard Vanbrabant, *La propriété Intellectuelle. Tome 1 – Nature Juridique, Création Information Communication* (Larcier, 2016) pp. 159 et seq.

extent that ownership would apply, given the *a priori* absolute character of ownership rights, the owner may *a priori* prohibit any act affecting their patrimony without exceptions (e.g. for private use) or time restrictions that the owner would have to consider. This is, of course, under reservation of other acts regarding the protection of the data carrier itself, in which the unstructured data would be incorporated, and possible qualification as ICT crimes.

As a consequence, it seems that, to date, no specific solid solution exists if a copy is made of unstructured data that is not protected by any IP right and that, in such a case, one could depend on the creativity of the courts to apply property concepts in a stricter or more progressive way.

In any event, unstructured data can be subject to any contract (sale, right to access, etc.), irrespective of the applicable legislation (IP rights, civil law, etc.).

As IP rights, ownership (and property) rights can be subject to transfers (assignment, licence, etc.) as well as the underlying data. No specific rules in contract law are available for such transfers. Regarding property rights or data-related rights of access, use, re-use, etc., please note that there is no publicity system for a transfer of ownership regarding movable goods, among which unstructured data is included. However, as stated above, the public possession of a movable good in principle counts as a presumption of ownership, which makes a written agreement advisable for enacting a transfer for enforceability reasons (Article 2279 CivC).

v) Exceptions and Limitations

The legislation on property rights does not contain specific exceptions or limitations regarding the use of unstructured data, such as for data mining or use of data for scientific research or a limitation on destroying such unstructured data.

In the future, exceptions similar to those found in Directive (EU) 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market (Directive 2019/790) for text and data mining may have to be considered as exceptions to rights other than copyright. Reference is made in this respect to Recital 9 Directive 2019/790, which provides that 'text and data mining can also be carried out in relation to mere facts or data that are not protected by copyright, and in such instances no authorization is required under copyright law'.

b) IP Rights

i) General

Considering the (very) broad scope of the concept of unstructured data as defined above (*see* section 1), it cannot *a priori* be excluded that unstructured data may be protected under one and/or another IP right provided, of course, that the corresponding conditions for protection are met. However, it should be pointed out at the outset that given unstructured data is by definition *unstructured*, it cannot qualify as a database and therefore cannot be protected as such, either by copyright or by the *sui generis* right of databases. This being said, from a theoretical point of view, it is not impossible that unstructured data may satisfy the conditions of protection relating to other IP rights, including:

- Copyright, which protects an original work (or creation);
- Trade mark law, which protects a distinctive sign used by an economic operator in order to identify their goods and services to consumers and, in so doing, to distinguish them from those of other economic operators;
- Design law, which protects the outward appearance of a product.[18]

From the outset, it should be noted that although the trade secret protection regime is largely inspired by the IP rights protection regime, trade secrets are distinct from (and do not qualify as) IP rights in that, in particular, they do not confer on their holder an exclusive right of ownership. Therefore, unlike an IP rights owner, the trade secret holder cannot prohibit *any* third party from using the information covered by their trade secret; they can only oppose the unlawful acquisition, use and/or disclosure of the trade secret, whereas the law expressly identifies a number of acts against which the holder cannot oppose even if those acts are likely to undermine the trade secret (*see* section 4).

Since the purpose of this contribution is not to provide an in-depth review of the various IP rights regimes, but only to examine if unstructured data may be protected under IP rights, we will only briefly review some of the IP rights that may protect unstructured data and, more specifically, the conditions for such protection, the owner of the resulting rights, the scope of the rights conferred and the exceptions to and limitations on those rights.

ii) Requirements for Protection

As indicated above, only some of the relevant IP rights concerning unstructured data will be discussed below:

- To be protected by *copyright*, a work must result from a creative activity, be put into form, and be original. These conditions do not imply any requirement for the work to be of a certain artistic and/or aesthetic nature, to have a certain size, a certain value, etc. The notion of work must be understood in the broadest sense of the term and could therefore, in theory, be applied to unstructured data.
- A work is automatically protected as soon as the above conditions for protection are met. It is therefore not necessary to carry out any formality for a work meeting these conditions to be protected by copyright (Article XI.165 of the Belgian Code of Economic Law (CEL)).
- For a sign to qualify as a *trade mark* and be eligible for protection as such, it must be distinctive, lawful and available, and capable of being represented on the register (Article 2.1 of the Benelux Convention on Intellectual Property (BCIP) and Article 4 of the Regulation (EU) 2017/1001 of 14 June 2017 on the European Union trade mark (Regulation 2017/1001)). Apart from signs expressly excluded from protection under trade mark law, there are virtually no restrictions as to the nature of the sign that may serve as a trade mark (words, logos, letters, numerals, shapes, colours, sounds, etc.), provided that it fulfils the conditions set out and, more particularly, that it has the capacity to fulfil the role of a trade mark (i.e. indicating the commercial origin of the goods and services covered). It cannot therefore be excluded *a priori* that unstructured data may qualify as a trade mark.
- A sign satisfying the cumulative conditions laid down to that effect will only be effectively protected as a trade mark once it has been registered in the corresponding register for the goods and services for which it is (intended to be) used. It is therefore not sufficient to be the first to have created and/or used a particular sign in order to benefit from the trade mark right relating to it, but one must be the first to have registered it.
- To be protected, a *design* must be new and have an individual character, independently of any aesthetic requirement (Article 4 of the Council Regulation (EC) 6/2002 of 12 December 2001 on Community designs (Regulation 6/2002)). Apart from the features relating to the appearance of a product that are expressly excluded from protection by design law, there are almost no restrictions as to the nature of the appearance features that may be protected and/or as to the product incorporating those features. Therefore, it cannot be excluded *a priori* that unstructured data may qualify as a design and be protected as such.
- At the Benelux level, the right to a design arises exclusively from the registration of the design (Article 3.1 BCIP), whereas at the EU level, it is possible to avail oneself of both a registered and an unregistered design (Article 4 Regulation 6/2002), the choice of one or the other having consequences in particular on the scope of the rights conferred and the term of protection.

iii) Owner

Both a natural person and a legal entity can be the holder of an IP right, both alone or in co-ownership.

Below, we briefly review some of the specificities of IP rights that may protect unstructured data:

- The original owner of a *copyright* in an original work is in principle the author, i.e. the natural person who created the work (Article XI.170, paragraph 1 CEL). However, the law provides that, in the absence of proof to the contrary, any person (natural or legal) who appears as such on (a reproduction of) the work or in connection with a communication to the public of the work, by reason of the statement of their name or an abbreviation allowing them to be identified, will be presumed to be the author (Article XI.170, paragraph 2, CEL). However, this presumption is rebuttable and may only be invoked against the original author in writing (even in the case of a work created in execution of an employment contract or on commission – Article XI.167, paragraph 1, CEL).

18. Patent rights, which protect an invention, will be dealt with in section 2. c). It should be noted from the outset that this differentiated treatment of patent rights (compared to other relevant IP rights) is not, in Belgium, justified by any specificity of this particular IP right in relation to the subject matter of the present contribution (i.e. unstructured data), but aims at ensuring a certain coherence in the structure of the different contributions of this book.

- The *trade mark* holder is the person (natural or legal) who appears as such in the relevant trade mark register.
- The *design* right belongs to its creator, who is a natural person, or to the creator's successor in title. If the design is created by an employee in the course of their employment, then the right to the design belongs to the employer, unless otherwise agreed (Article 14.2 Regulation 6/2002; Article 3.8 BCIP). In Benelux, the same presumption applies in the case of a design created on commission in favour of the commissioning party, 'provided that the commission was given with a view to commercial or industrial use of the product in which the design is incorporated' (Article 3.8.2 BCIP).
- In the case of a registered design (Benelux or Community design – *see* above), the holder is expressly identified in the relevant register.

In the light of the above, we note that, unlike property rights, there is no doubt that the rule set out in Article 2279 CivC (Article 3.28 new CivC), according to which public possession of movable goods count as a presumption of ownership, does *not* apply to IP rights since they are subject either to an obligation of registration in a public register, or to a presumption of ownership, or to some other specific requirements.

iv) Scope of Protection

While property rights are in principle absolute and perpetual, IP rights are not. An IP right confers exclusivity only for a limited period of time (i.e. the period of validity of the IP right in question) and offers a monopoly to the holder only for certain specific acts of exploitation, which are moreover subject to certain exceptions and limitations provided for by law.

Below is a non-exhaustive overview of the main acts reserved for the IP rights owner:

- *Copyright* includes in particular the right to reproduce the work (including the right to authorize its adaptation or translation, rental or loan), to communicate it to the public and to authorize its distribution to the public, by sale or otherwise (Article XI.165 CEL). This right arises from the sole creation of the original work and continues for 70 years after the death of the author for the benefit of the person that the author has designated for this purpose or, failing this, the author's heirs (Article XI.166, §1, CEL).
- The proprietor of a *trade mark* has the exclusive right to use the trade mark in the course of trade for goods and/or services covered by the trade mark for a period of ten years, which may be renewed indefinitely (Articles 9 and 10 Regulation 2017/1001; Article 2.20 BCIP).
- A registered design confers on its holder the exclusive right to use it for products identical or similar to those in which the design is incorporated or applied, for a period of five years, extendable up to a maximum of 25 years (Article 3.16 BCIP; Articles 12 and 19.1 Regulation 6/2002). An unregistered Community design is protected for a period of three years only (Articles 11 and 19.2 Regulation 6/2002).

In addition to the above-mentioned exploitation rights, the IP rights owner may in principle freely transfer their rights (e.g. by way of assignment or licence), in whole or in part, for the entire legal term of protection or only for part of it, etc. In certain specific cases, the IP rights owner will however have to comply with a certain number of formalities, which sometimes condition the validity of the transfer in question and sometimes its opposability against third parties. These include:

- The *copyright* owner may assign and/or license all or part of their economic rights, subject to the conditions strictly enumerated by the law with regard to contracts concluded by the original authors (against which any transfer must necessarily be proven in writing and must contain specific specifications on pain of nullity). The original author may however not transfer their moral rights to their work.
- Any assignment (total or partial) of a *trade mark* must be made in writing on pain of invalidity (Article 2.31.2 BCIP and Article 20.3 Regulation 2017/1001) and must be entered in the corresponding register in order to be opposable against third parties (Article 2.33 BCIP and Article 27 Regulation 2017/1001). It should be noted that, in order to be valid, the assignment of a Benelux trade mark must necessarily cover the entire Benelux territory. The grant of a licence need not necessarily be in writing, but must be recorded in the trade mark register in order to have effects vis-à-vis third parties.
- Any assignment of a *design* must be made in writing, on pain of nullity, and, where it concerns a Benelux design, for the entire Benelux territory (Article 3.25.2 BCIP). In addition, for the assignment to be opposable against third parties, an extract of the deed recording the assignment must be registered with the corresponding office (Article 3.27 BCIE and Article 33 Regulation 6/2002). The grant of a licence on a design need not be in writing, but must be registered in order to have effects vis-à-vis third parties.

The exclusive rights identified above have as a corollary the right to prohibit an unauthorized third party from carrying out such acts and, correlatively, to prosecute any such infringement.[19]

v) Exceptions and Limitations

In addition to the limitations inherent in the principle of Community exhaustion – which applies to all IP rights – an IP rights owner's rights are subject to certain exceptions and limitations exhaustively enumerated by law, such as, in particular:

- In specific cases, users do not have to expressly request permission from the *copyright* owner to reproduce or communicate the protected work to the public. These exceptions and limitations can be grouped into the following categories:

19. For the sake of completeness, we note that the prohibition right of the holder of an unregistered community design is limited to the use of a copy of the protected design (Art. 19, paragraph 2, Regulation 6/2002).

- exceptions in favour of teaching and/or scientific research (quotation of an excerpt from a work for the purposes of criticism or teaching; anthologies of works intended for teaching; reproduction and communication of works as part of school activities and/or to illustrate teaching or research; etc.);
- exceptions for libraries, museums and archives (consultation of works on library or museum terminals; copies of works for the preservation of cultural and scientific heritage; etc.);
- exceptions for private use (communication of works in the private or family sphere; copies of works for personal use only, etc.);
- exception for reprography (i.e. making photocopies (of fragments) of works in the context of professional activities);
- exceptions in favour of information (reproductions of works located in a public place when the reproduction of the work is incidental and does not constitute the main purpose of the reproduction; caricature, parody or pastiche, made for humorous purposes; reports of current events relating to the work concerned; etc.);
- other exceptions (copying and adaptation of a work in order to enable a disabled person to have access to it; temporary reproductions of works made automatically in the digital environment; panorama exception; etc.).
- *de lege ferenda*, an explicit exception regarding text and data mining will be provided for when implementing Directive 2019/790.[20]

– The *trade mark* owner may not oppose:
  - subject to honest practices in industrial or commercial matters, the use of their trade mark by a third party for information purposes (i.e. indications relating to their name and address; indications relating to the characteristics of the third party's goods or services; indications necessary to inform as to the intended purpose of a product or service, in particular as an accessory or spare part – *see* Articles 2.23.1 BCIP and 14.1 Regulation 2017/1001);
  - the use of a sign that was already locally used prior to the registration of the trade mark (e.g. a trade name);
  - the use of a subsequent registered similar trade mark (not an unregistered sign) against which the owner has not taken any action during an uninterrupted period of five consecutive years.
– The exclusive right to a *design* (registered or unregistered) does not imply the right of the holder to object to:
  - acts performed privately and for non-commercial purposes;
  - acts carried out for experimental purposes;
  - acts of reproduction for illustration or teaching purposes;

20. Pursuant to Art. 2.2 Directive 2019/790, 'text and data mining' means any automated analytical technique aimed at analysing text and data in digital form in order to generate information that includes but is not limited to patterns, trends, and correlations. Arts. 3 and 4 Directive 2019/790 provide for several exceptions for text and data mining, e.g. for scientific research, teaching activities and cultural heritage.

  - the use of the protected design constituting a part of a complex product for the purpose of repairing that product;
  - the use of products that have an identical appearance to the design (or which do not produce a different overall impression on the informed user) that were manufactured before the date of filing of the design in question.

In the first three scenarios, the third party making use of the protected design will always have to indicate the source of the design in question.

c) Patent Rights

i) General

As mentioned in footnote 18, patent rights are one of the IP rights that can protect unstructured data, provided of course that the conditions for protection are complied with. In this section we will briefly examine the conditions for such protection, the owner of the rights that may result therefrom, the scope of the rights conferred, and the exceptions and limitations to patent rights. However, we will not review the general rules and principles applying to all IP rights (community exhaustion, the fact that the exclusive rights specific to a given IP right always have as a corollary the right to prohibit an unauthorized third party from carrying out such acts, etc.), and we refer you in this respect to the previous section 2. b).

ii) Requirements for Protection

To be patentable, an invention must be new, involve an inventive step, be susceptible of industrial application, and be lawful (Article XI.3 CEL).

The law expressly identifies a number of items that may not be regarded as inventions, while it also identifies certain items excluded from patentability. As long as it does not fall into either of these two categories, it cannot be excluded *a priori* that unstructured data may qualify as a patentable invention. However, if this is the case, then such an invention will only be protected as a patent after it has been registered.

iii) Owner

In principle, the right to apply for a patent and the subsequent right to the patent benefits the inventor, who is a natural person. However, the inventor may assign their right to apply for a patent or, subsequently, the obtained patent (Article XI.9 CEL). In any case, both the inventor and the owner of the patent will be identified in the patent register.

For the sake of completeness, we note that the general law does not provide for a general rule of presumption of ownership in favour of the employer or the commissioning party. Unless this matter is regulated by specific legislation, it will in principle have to be settled by contract. However, in the event of a dispute, and in the absence of a clear contractual solution, the courts sometimes decide to attribute the right to apply for the patent or the obtained patent to the employer or to the

commissioning party, taking into account the circumstances in which the invention was created (i.e. in the exercise of a contract, on the instructions of, using the means made available by, etc.).

iv) Scope of Protection

A patent confers on its proprietor the exclusive right to exploit the invention – except for reasons of public order and security – for the entire term of protection (Articles XI.3 and XI.29 CEL), i.e. for twenty years from the date of filing of the patent application, a term which, in the case of medicinal and plant protection products, may be extended to a maximum of 25 years and 6 months by means of supplementary protection certificates.

Both the assignment and the grant of a licence on a patent must be made in writing on pain of nullity (Article XI.50, §2, and Article XI.51, §1, CEL). Moreover, they will only be enforceable against third parties if they are entered in the relevant patent register (Article XI.50, §6, and Article XI.51, §6, CEL).

Eventually, it is noteworthy that in patent matters, the applicant is also able to take action against an unauthorized third party before the patent is effectively granted (but after publication of the application). If the patent is ultimately not granted or if it does not cover the specific exploitation made by the third party, then the third party will be able to claim restitution of the compensation paid.

v) Exceptions and Limitations

The patent owner may not oppose:

- acts performed in a private context and for non-commercial purposes;
- acts carried out for scientific purposes on the subject matter of a patented invention and/or by means of that invention;
- the preparation by and sale in pharmacies of medicine protected by a patent, provided that the medicine is intended for individual use and is supplied on medical prescription;
- acts of use, in good faith, of a product or process prior to the grant of the patent;
- the granting by the public authority of a compulsory licence in the scenarios defined by law.

3. CONTROL OVER DATA BY CONTRACT INCLUDING BOUNDARIES FOR CONTRACTUAL RULES

In addition to possible protection by (IP) property rights, unstructured data could be protected by contract. As a contract prevails between parties, the parties concerned can in principle freely deal with unstructured data and, in so doing, they can establish either a form of ownership in data or a set of data-related rights, of which they are free to define the scope. In this respect, some legal scholars also refer to contracts as establishing either a *de facto ownership* or a *direct control* over data, irrespective of whether it is actually enshrined in the CivC.

In Belgium, there are no contractual rules specific to unstructured data. Contracts relating to unstructured data are therefore subject to general contract law, which in principle confers the greatest freedom upon the parties, subject to, of course, mandatory rules and the rules of public order and the general governing legal principle to perform obligations and execute contracts in good faith (Articles 1134 and 1135 CivC).

4. OTHER FORMS OF LEGAL PROTECTION CONTROLLING ACCESS TO, AND USE AND DISSEMINATION OF UNSTRUCTURED DATA

a) Trade Secrets

i) Background

Independently and, in some cases, in addition to the protection that may be put in place by contract, unstructured data may be protected as a trade secret. Indeed, as potentially *any* type of information could be protected as trade secrets (*see* below), it is commonly accepted that unstructured data can *a priori* qualify as a trade secret, provided of course that it meets the conditions set out in this respect.

In Belgium, the legislator implemented Directive (EU) 2016/943 of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (Directive 2016/943) on 30 July 2018 in national legislation.[21] Since a few provisions of different pieces of legislation already allowed for the protection of trade secrets, the Belgian legislator decided to amend the existing texts (mainly the CEL, the Belgian Judicial Code (JudC) and the Belgian Act of 3 July 1978 on employment contracts (AEC)) instead of adopting one single autonomous act.

From the outset, we note that while the trade secrets protection is largely inspired by and, in practice, similar to the protection of IP rights, trade secrets do not constitute a new IP right, but fall within the field of unfair competition. Trade secrets inherently differ from IP rights, as the information covered by the trade secret is not strictly speaking the *property* of its holder, unlike an IP right which, once granted, is literally the (intellectual) *property* of its holder (at least for a specific period of time). Correlatively, and again in contrast to IP rights, trade secrets do not confer on their holder an exclusive right of prohibition, but only establish rules of good conduct (similar, and expressly echoing, the unfair practice law) aimed at preserving the confidentiality of information of commercial value and, correlatively, at punishing any act of acquisition, use and/or disclosure carried out in breach of those rules.[22]

21. *See* Belgian Act of 30 July 2018 on trade secrets protection (M.B., 14 August 2018), http://www.ejustice.just.fgov.be/eli/loi/2018/07/30/2018031595/justel (accessed on 1 March 2021).
22. Hendrik Vanhees, 'De Nieuwe Wettelijke Regeling Betreffende de Bescherming van Bedrijfsgeheimen', *R.W.* (2018-2019) p. 1642.

information is not subject of a proprietary right, and its taking could not resulting in a person being deprived of property.[3] However, there may be equitable rights that arise from either the relationship of the parties in relation to each other and the data, or enforceable contractual rights. See the discussion below.

These equitable rights, such as the right to protect confidential or secret information, the right to control access and use through contract, are rights but they are perhaps not property rights *per se* as they are not always freely transferable or alienable.

b) IP Rights

As discussed above, data may be protectable under copyright as a 'compilation' but only if the database is 'original' and the result of skill and judgment in the selection and arrangement of the data and the act of compilation is not a mere mechanical exercise. This is likely to be the case with some databases but almost certainly not the case with unstructured data.

The Copyright Act provides that copyright exists for 'every original literary, dramatic, musical and artistic work'.[4] This phrase is defined at section 2 to include compilations, which is in turn defined to include works 'resulting from the selection or arrangement of data'. In *Toronto Real Estate Board v Commissioner of Competition*[5] the classification of the database of house prices as a compilation was not contested by either party on appeal. However, the Court found that the evidence of the Toronto Real Estate Board did not speak to skill and judgment in compiling the database, but rather the evidence showed that the collection was a mechanical exercise and that therefore copyright did not attach to that database.

However in *Geophysical*, the Alberta Court of Queen's Bench held that copyright can subsist in seismic data of the following kind, namely:

(i) raw seismic field data, or raw seismic, magnetic, and gravity data;
(ii) seismic related navigation data;
(iii) processed and reprocessed seismic data;
(iv) selections, arrangement and compilations of raw, processed and reprocessed seismic data;
(v) productions and reproductions of seismic data in various forms and media including physical, electronic, magnetic and digital works;
(vi) interpretations, derivations and translations of the seismic data; and
(vii) related seismic data materials.[6]

The meaning of the word 'original' in section 5 of the Copyright Act was considered by the Supreme Court in *CCH Canadian Ltd. v Law Society of Upper Canada*,[7] [*CCH*]:

3. *R. v Stewart*, SCC, 50 D.L.R. (4th) 1.
4. Copyright Act, R.S.C. 1985, c. C-42, section 5.
5. 2017 FCA 236.
6. *Geophysical Service Inc. v Encana Corp.* (2016), 2016 CarswellAlta 742, 2016 ABQB 230, [2016] 10 W.W.R. 111, 38 Alta. L.R. (6th) 48.
7. 2004 SCC 13, [2004] 1 S.C.R. 339.

> 'For a work to be "original" within the meaning of the Copyright Act, it must be more than a mere copy of another work. At the same time, it need not be creative, in the sense of being novel or unique. What is required to attract copyright protection in the expression of an idea is an exercise of skill and judgment. By skill, I mean the use of one's knowledge, developed aptitude or practised ability in producing the work. By judgment, I mean the use of one's capacity for discernment or ability to form an opinion or evaluation by comparing different possible options in producing the work. This exercise of skill and judgment will necessarily involve intellectual effort. The exercise of skill and judgment required to produce the work must not be so trivial that it could be characterized as a purely mechanical exercise. For example, any skill and judgment that might be involved in simply changing the font of a work to produce "another" work would be too trivial to merit copyright protection as an "original" work.'

In *Distrimedic Inc. v Dispill Inc.*,[8] the Federal Court held that 'when the content and layout of a form is largely dictated by utility and/or legislative requirements, it is not to be considered original' (at para. 324). Indeed, the Copyright Act specifically provides that it is not an infringement of copyright to apply to a useful article features that are dictated by a utilitarian function.[9]

That copyright need not extend to mere data is also a result of the TRIPS Agreement (Article 10(2) which does not require extending copyright protection to the data or subject matter itself:

> '10(2) Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, *which shall not extend to the data or material itself*, shall be without prejudice to any copyright subsisting in the data or material itself.' (Emphasis added.)

c) Patent Rights

The grant of a patent requires an invention, i.e. something which is not obvious to an ordinary skilled workman skilled in the art. In addition, patents are granted only for any new and useful 'art, process, machine, manufacture or composition of matter'.[10] Unstructured data standing alone would not be considered any of these. However, the method of collecting unstructured data could be an invention if there is something novel and inventive about its extraction or use. In one case, the Canadian Federal Court of Appeal has held that claims to an apparatus for processing well logging data was not patentable and there was no suggestion that the data itself would be patentable.[11] However, the Canadian Patent Office has found that a system and method for updating and distributing data for in-vehicle navigation systems is patentable.[12] However, again, the novelty and inventiveness are in the system of collection and

8. 2013 FC 1043, 440 F.T.R. 209.
9. Copyright Act section 64.1.
10. Patent Act, R.S.C. 1985 c. P-4, section 2.
11. *Schlumberger v Commissioner of Patents* (1981) 56 C.P.R. (2d) 204 (F.C. A.).
12. *Navigation Technologies Corporation's Application* 2,195,252 (2012) CD 1332.

extraction and possible use and not in the data itself. If the use of the data is a patentable method, then it is possible that data could be indirectly protected when used by or in the patented method. However, the Patent Act specifically provides that 'no patent shall be granted for any mere scientific principle or abstract theorem'.[13] It was this section that was applied in the *Schlumberger* case mentioned above in denying a patent for the collection and use of well logging data. On the same basis, most business methods have been denied patents on the basis that they represent mere manipulation of numbers.

3. CONTROL OVER DATA BY CONTRACT INCLUDING BOUNDARIES FOR CONTRACTUAL RULES

Access to, and use and dissemination of data can be controlled by contract. In general, access to data generated by an individual can be restricted by that individual by contract.

Under common law rules, contracts that are in restraint of trade may be unenforceable if they are not reasonable between the parties and reasonable in the public interest. It would likely be difficult to render a contract relating to the use of data unenforceable on common law grounds if it is a commercial contract between parties dealing at arm's length.

However, contracts dealing with data are subject to the same legal rules as any other contract. For example, contracts (and indeed other behaviour) relating to the use of data are subject to the same rules that govern bargaining in good faith and anticompetitive behaviour under the Competition Act.[14] See the discussion at point 5 below.

The party to a contract who receives data under the terms of a contract is prohibited from doing anything that is contrary to the terms of the contract. Breach of contract by one party will entitle the opposite party either to an action for damages, or in some circumstances to such equitable remedies as specific performance or an injunction.

4. OTHER FORMS OF LEGAL PROTECTION CONTROLLING ACCESS TO, AND USE AND DISSEMINATION OF UNSTRUCTURED DATA

Trade secret protection is available where the data is truly secret. Data which is not entirely secret but which is available only to those who owe a duty of confidence may also be protected in equity by an action for breach of confidence which may be used to prevent disclosure of the confidential information when the data and the relationship between the parties meet certain conditions.

The Supreme Court of Canada in *Lac Minerals*[15] has recognized the elements of breach of confidence as requiring that:

13. Section 27(8).
14. Competition Act, R.S.C. 1985, c. C-34.
15. *International Corona Resources Ltd. v Lac Minerals Ltd.*, [1989] 2 S.C.R. 574, 61 D.L.R. (4th) 14.

(a) The information must have the quality of confidence;
(b) The information must be imparted in circumstances in which an obligation of confidence arises; and
(c) There must be an unauthorized use of the information to the detriment of the Plaintiff.

The person entitled to enforcement of a right in the confidential information will be a party to a contract or in some cases a party to a relationship where an obligation of trust or confidence is known to arise in a situation where the information was disclosed in violation of the obligation of confidence.

Misuse of confidential information is prohibited by the breach of confidence right. This likely includes the disclosure of the unstructured data in a manner that harms the owner of the information. Misuse can occur even where the information is not disclosed to a third party. In addition, if a contract concerning the confidentiality of the mere data exists, breach of contract for any specifically prohibited uses of the information may also be possible.

Article 39, Trade Related Intellectual Property Agreement[16] (TRIPS) to which Canada is a party, would support, or even require, protection for trade secrets and confidential information by extending the need for protection beyond 'disclosure' or the 'imparting' of 'undisclosed information' to improper acquisition in 'a manner contrary to honest commercial practices'.[17]

Article 39(1) and (2) TRIPS is in the following terms:[18]

> '1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.
>
> 2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices[19] so long as such information:
> (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
> (b) has commercial value because it is secret; and

16. 'Agreement on Trade-Related Aspects of Intellectual Property Rights' Annex 1C to 'The Agreement Establishing the World Trade Organization' ('WTO Agreement').
17. *See* R. Howell, *Database Protection and Canadian Law* (2d ed., 1998), prepared for the Department of Canadian Heritage, online: http://publications.gc.ca/site/archivee-archived.html?url=http://publications.gc.ca/collections/Collection/C2-370-1998E.pdf.
18. Article 39, TRIPS Agreement.
19. For the purpose of this provision, 'a manner contrary to honest commercial practices' shall mean at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition.

The Federal and Provincial Governments can and do assert Crown Copyright in works prepared by them and in works prepared or published by or under the direction or control of Her Majesty or any government department. Pure data is likely not a 'work' but the compilation or arrangement of data may be a 'work' and therefore would be subject to copyright. Unless otherwise permitted by law or specified in the publication in issue, Crown copyrighted works may be reproduced by those outside of the Federal Government provided prior permission is secured in writing. The Crown has announced a blanket permission to reproduce statutes or judicial decisions without charge and without prior permission.

Recently the Supreme Court of Canada upheld Crown copyright in surveys created by land surveyors and deposited in the land registry office.

The Public Servants Disclosure Protection Act provides that the Public Sector Integrity Commissioner may not disclose any information that the Federal Government or a portion of the public sector is taking measures to protect. This includes information reasonably expected to harm commercial interests. However, a public interest exception permits such disclosure if it is in the public interest and the benefits of disclosure clearly outweigh the potential harms.

Government information can be accessed through an access to information request. Records, regardless of the format, include those held under the control of a Federal Government institution. Some types of records are excluded, including Cabinet documents, information relating to national defence and security, law enforcement, and personal information concerning other individuals, and confidential information of third parties.

b) Privacy

The collection, use and disclosure of personal data is regulated by both Provincial and Federal law. In this summary we review only the law in Ontario and Canadian Federal law. Individual provinces have similar provisions and should be consulted.

The Federal Personal Information Protection and Electronic Documents Act[27] (PIPEDA) requires that individuals consent to the collection, use, and disclosure of their personal information (sch. 1, clause 4.3.1). This consent must be informed (sch. 1, clause 4.3.2). Amendments in 2015 to this principle specified that for consent to be informed, the person must understand the 'nature, purpose and consequences of the collection, use or disclosure of the personal information' (s. 6.1).

PIPEDA only requires new consent where information is used for a new purpose.

In *TREB*,[28] the Federal Court of Appeal agreed that privacy rules mandated by PIPEDA must be followed where it relates to the release of personal data in relation to house prices but concluded that there was sufficient evidence of consent by those persons whose information had been disclosed by the real estate board.

However, it is clear that PIPEDA can extend to personal information which could include information such as financial information, the sale prices of articles and personal income. Under the most recent amendment to PIPEDA: '"personal information" means information about an identifiable individual, but does not

27. S.C. 2000, c. 5.
28. 2017 FCA 236.

include the name, title or business address or telephone number of an employee of an organization.'

Health data is also separately regulated (see below).

c) Health Data

There are a number of specific rules relating to health data related to regulatory approval and personal health data.

i) Health Data for Regulatory Approval

New medicinal products are eligible for data exclusivity (which Canada calls 'data protection') if certain criteria are met.

The practical effect of Canada's data protection regime is to extend the period of market exclusivity for originators of new drugs. In Canada, generic companies support their applications for regulatory approval for a generic version of a previously approved drug by referencing the data on the safety and efficacy filed by the originator of that drug. Generic companies can reference the data submitted by the originator company, but cannot itself access this data.

Canada's data protection regime provides that no subsequent-entry product may apply for an application for regulatory approval referencing the data of a previously approved product until six years after the issuance of the originator's regulatory approval. The Minister of Health must also wait an additional two years before issuing an approval to the subsequent entrant. If the originator submits eligible pediatric data within the first five years of the eight-year period, the originator can obtain an additional six months of data protection.

The practical effect is eight years of protection of data (and thus market exclusivity), with a possible six-month extension.

Data protection is only available when the following criteria are satisfied:

a) The dossier of protected data must relate to an 'innovative drug', that is a drug containing an active medicinal ingredient not previously approved in a drug in Canada, and not a variation of a previously approved medicinal ingredient such as a salt, ester, enantiomer, solvate or polymorph. If the medicinal ingredient has been previously approved, it is not eligible for data protection.
b) The applicant must have gone to considerable effort to generate the data that supports the approval. Generally, evidence of the safety, efficacy, properties, and conditions of use of the drug from the applicant's clinical studies satisfies these criteria, while evidence from the literature, studies by others and/or market experience does not.

The data submitted by an originator company was traditionally not available to the public unless the company itself chose to make it so. This is changing. Now, within 120 days of a decision, Health Canada will post clinical study reports on a new government online portal, starting with drugs that contain novel active ingredients and adding devices and other drugs over a four-year phase-in period.

Act or the provisions issued thereunder. Data may be inspected and a copied, but the trader will maintain its right to defence under section 38. According to section 38(3) the trader is not obliged to submit to the Competition and Consumer Agency documents containing confidential correspondence between an external legal adviser and the client.

6. SPECIFIC RULES FOR SPECIFIC DATA

In addition to what has been discussed above in this article, various other forms of legal protection are potentially available for unstructured data in Finland and the body of legislation affecting its use, dissemination or access to it is vast. Relevant provisions can be found in civil, administrative and criminal laws, and much of the relevant legislation is sector-specific and only applicable to certain types of data.

As discussed above, the legislation that protects trade secrets and restrictions on the use of personal data have been harmonized with EU legislation to great extent and there are overlaps between EU and Finnish legislation also on a very fundamental level. By way of example, as regards the protection of personal data and privacy, the fundamental right to privacy covers the protection of data, stemming from inter alia the European Charter of Human Rights (Article 7)[50] whereas in the Finnish Constitution (731/1999, in Finnish: *Suomen perustuslaki*) the right to privacy is covered in section 10. Pursuant to section 10(1), 'everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act'. Furthermore, section 10(2) specifically states that the secrecy of a letter, a phone call and other confidential messages is inviolable.[51]

Privacy and protection of personal data is heavily regulated. In addition to the GDPR, numerous national general and sector-specific acts cover the protection of personal data. The GDPR and the national Data Protection Act are complementary and govern the use and handling of personal data on a general level. Most of the sector specific laws are applicable alongside the GDPR, but there are laws such as the Act Processing of Personal Information in Criminal Matters and National Security Matters (1054/2018) and Act on Processing of Personal Information in Immigrant Administration (615/2020) that contain sections that will be applicable instead of general legislation. On estimation, over 700 differed national laws contain provisions on the direct or indirect protection of personal data (regardless of whether such data is structured or unstructured), and it is not possible to exhaustively describe all the relevant legislation within the ambit of this chapter.[52]

50. *See e.g.* European Data Protection Supervisor, *Data protection*, https://edps.europa.eu/data-protection/data-protection_en, (visited 12 February 2021).
51. *See* e.g. Maria Wasastjerna, *Competition, Data and Privacy in the Digital Economy: Testing Conventional Boundaries and Expanding Horizons – Towards A Privacy Dimension in Competition Policy?* (Kluwer Law International, 2020) p. 46.
52. Olli Pitkänen, 'Tietosuojasäädösten muutostarve', *Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja* (7 June 2017), http://urn.fi/URN:ISBN:978-952-287-389-7 (visited 12 February 2021).

As the administration and exercise of public power is based on law, the legislative measures are many which results in great number of laws affecting also use, processing and dissemination of unstructured data. The Act on the Transparency of Government Activities (621/1999, as amended, in Finnish; *laki viranomaisten toiminnan julkisuudesta*) regulates the secrecy and confidentiality of official documents in general. It contains sections for example on handling of documents containing information on private trade secrets (chapter 6, section 24). Open and transparent administration is a general principle, but some matters require more sensitivity. This chapter provides selected illustrative examples of sector specific national laws relevant to the subject.

a) Public Data

The EU has had legislation on availability of public information since 2003. The previous directive on public sector information[53] was implemented in the Act on the Transparency of Government Activities, Act on Criteria for Charges Payable to the State, and the Act on Sovereignty of the Island of Åland. The national implementation of the renewed Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast) ('Open Data Directive') is currently in progress and scheduled to be completed by 17 July 2021.[54]

Prior to the Open Data Directive, there has been no general legislation concerning re-use of information although various sector specific laws have provided access to public sector information. The Ministry of Finance has also taken action to publish data and interoperability tools with open licences. The Ministry of Finance coordinates public sector ICT matters. It has conducted an Open Data Programme to create and publish a portal for open public data as a part of its information policy and steering. The portal is also the source where material is harvested to the European Open Data Portal.[55]

The new Open Data Directive requires producing and releasing data in certain formats and provides processes for responses to data requests, which have been absent in the previous laws and other measures on data information management in public administration. Open Data Directive also introduced classification of certain data as a 'high value data set' , which is a novelty. New processes are required and the already taken voluntary measures are insufficient to meet the requirements of the Directive. In order to implement the Directive, Finland will amend the Act on Information Management in Public Administration during 2021 and enact two new laws on the re-use of data. There will be an Act on Re-use of Data in Certain Public Enterprises, and an Act on Re-Use of Research Material Produced with Public Funds.

53. Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information.
54. Government proposal *Hallituksen esitys avoimen datan direktiivin täytäntöönpanoa koskevaksi lainsäädännöksi*, available at https://vm.fi/hanke?tunnus=VM100:00/2020 (visited 12 February 2021).
55. Opening up access to data for innovative use of information, https://vm.fi/en/opendata (visited 15 February 2021).

b) Employment

Protection of personal data extends also to the workplace. The Finnish Act on the Protection of Privacy in Working Life (759/2004, as amended, in Finnish: *laki yksityisyyden suojasta työelämässä*) applies to the processing of employees' personal data. Section 3(1) of the Act lays down a necessity requirement, according to which the employer is only allowed to process personal information directly connected to the employee's employment relationship. In addition, section 4(1) requires that personal data is to be collected primarily from the employee, or if this cannot be done then consent of the employee must be obtained. The Act on the Protection of Privacy in Working Life also contains rules on the possibility of an employer to monitor employees. Interestingly similar rules are absent in schools. All documents are public in any educational institutions unless the documents are subject to non-disclosure obligations. In such case, the school or educational Institute can collect and processes information on students but cannot disclose personal information to third parties. There are no rules on the primary source of information.

c) Electronic Communication Services Data

The Finnish Electronic Communications Services Act (917/2014, as amended, in Finnish: *laki sähköisen viestinnän palveluista*) contains rules on the processing of data. Chapter 17 section 137 identifies general processing principles of a communication intermediary. Under section 137(2), electronic messages and transmission data may only be disclosed to those parties who have the right to process the data in a particular situation. Section 137(3) adds that after processing, electronic messages and transmission data must be destroyed or the transmission data must be modified in a manner that it cannot be connected to the subscriber or user, unless otherwise provided by law.

In addition, the Finnish Electronic Communications Services Act covers *location data* based on the implementation the Directive on privacy and electronic communications (2002/58/EC).[56] Pursuant to chapter 20 section 160(1), location data that may be associated with a natural person can be processed for the purpose of providing and exploiting a value added service if the subscriber or user to whom the data relates has given his or her consent, or if the consent is apparent from the context, or if the law so provides. The government proposal for the Act further elaborates that location data can be utilized to determine, for instance, the accuracy of the location or the exact time the location information was saved.[57]

The infrastructure for spatial information is covered by the Finnish Act on Spatial Information Infrastructure (421/2009, in Finnish: *laki paikkatietoinfrastruktuurista*),

56. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector.
57. Government proposal HE 221/2013 vp, *Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta*, 89–89.

which implements the INSPIRE Directive 2007/2/EC[58] in Finland. The act covers 'spatial data' which means any data with a direct or indirect reference to a specific location or geographical area, as defined in Article 3(2) of the Directive and section 2(1)(1) of the Spatial Information Infrastructure Act.

d) Traffic Data

The Finnish Act on Traffic Services (230/2017 as amended, in Finnish: *Laki liikenteen palveluista*) demands open interfaces and availability of transport data. Chapter 18 discusses relevant data and requires that ticket and payment systems operate in a manner that smart traffic systems can be taken in use.

Section 154 of the Finnish Act on Traffic Services describes the framework that is established by the Finnish Transport Agency. It states:

> 'Irrespective of the mode of transport, the provider of a passenger mobility service shall ensure that relevant up-to-date information on the mobility service is available through a connection to the information system in a machine-readable and easily editable standard data format for free use (open interface). Relevant information includes at least route, stop, timetable, price, and availability information, as well as accessibility information.
>
> The web address or addresses of the interface referred to in subsection 1 and other data required for the use of the interface, as well as updates thereof, shall be notified to the Finnish Transport Agency before the commencement of operations or as soon as the new address is known.
>
> The Finnish Transport Agency shall provide a technical service with which the provision of information referred to in subsection 1 can alternatively be implemented.
>
> A Government decree may lay down more detailed provisions on the essential information referred to in subsection 1 and on the requirements for timeliness and technical interoperability.'

The traffic services are also harmonized to certain extent within EU with Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport ('ITS Directive'). ITS Directive introduced EU-wide Intelligent Transport Systems (ITS), which requires deployment of specifications standards to ensure interoperability between information and communication systems that are used in the field of transport, and to ensure smarter information services especially in the identified priority areas. Harmonization has been deemed necessary in the areas of optimal use of road, traffic and travel data; continuity of traffic and freight management; road safety and security applications; and linking the vehicles with transport infrastructure. The ITS Directive encourages the re-use of anonymous data and welcomes new applications and services to the extent personal data is protected.[59]

58. Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).
59. Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road

According to Section 160 of the Finnish Act on Traffic Services ('Deployment of intelligent transport systems') the principles established in Annex II of the ITS Directive are complied with when applying the specifications (Article 6) to the priority areas (Article 2) and to the measures defined in Article 3 of the ITS Directive. The Finnish Transport and Communications Agency shall assess and verify whether the priority service providers, organizations and other operators fulfil the requirements of the Directive and related other instructions. It will provide with further technical instructions for fulfilling such requirements if needed.

e) Banking and Financial Institutes

The secrecy of the banking matters is given in the Finnish Act on Operation of Credit Institutions (610/2014 as amended, in Finnish: *Laki luottolaitostoiminnasta*). According to chapter 15 section 14, any matter concerning the financial position or private circumstances, or business secrets of a customer shall be kept secret, unless the person whose secrets are being protected grants consent for disclosing the information. The obligation concerns persons who get the secret information while working directly or indirectly for or on behalf of a credit institution. The secrecy obligation prevents the disclosure of information also to the owners, shareholders and management of the credit institution. It is however also stressed that the secrecy obligation is not intended to prevent normal operation of the credit institute or stock market.[60] There are specific exceptions for disclosing the information within the same group of companies and to credit reference registers and other credit institutions. The disclosure criteria must be fulfilled, and the recipient has to be subject to similar secrecy obligations.[61]

The first and second EU Payment Service Directives[62] have been implemented by amending a great number of laws, including the Finnish Act on Payment Services (290/2010 as amended, in Finnish: *Maksupalvelulaki*), and by monitoring the measures that have been required from financial institutes. EU rules on opening the interfaces for payment service providers, data security and the strong electronic identification have caused plenty of amendments. Relevant legislation has been in force since 13 January 2018 but monitoring of some remaining obstacles related to certain special interfaces have also been done after the effective date.[63] EU harmonization of finance is not yet completed and new instructions and legislation will cause further amendments to the operation of banking and financial institutes, which is likely to affect the processing of data as well.

transport and for interfaces with other modes of transport. See. preamble, Arts. 1, 2, 3, 8, and 10.

60. Act on Operation of Credit Institutions (610/2014 as amended), chapter 15, Section 14.
61. Act on Operation of Credit Institutions (610/2014 as amended), chapter 15, Section 15.
62. Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (text with EEA relevance).
63. https://www.finanssivalvonta.fi/saantely/saantelykokonaisuudet/psd2/ (visited 12 February 2021).

Client registers in banks and financial institutions are subject to the GDPR, but the general and specific laws that govern the processing of information within the financial institutions do not provide an exhaustive view on the possibilities of third parties to access information that is protected under secrecy sections. Various different laws may grant the possibility to operate on behalf a legal person. There are rules on legal representation and in certain cases also family and inheritance law may provide grounds to provide an access to the secrets. Access to information may also be provided for persons who are responsible for accounting, for holders of securities, to some extent also for researchers and there are specific rules for representation in insolvency matters. Also, criminal investigation provides possibilities to gain access to the secret data.

f) Health Data

The Finnish Act on the Secondary Use of Health and Social Data (552/2019, in Finnish: *laki sosiaali- ja terveystietojen toissijaisesta käytöstä*) enables use of social and health data for statistics, scientific research, innovation and development activities, education, steering and supervision of health and social authorities, and for the planning and reporting the operations of the authorities. The Finnish Health and Social Data Permit Authority, Findata started its operations in January 2020. Findata actively promotes the secondary use of health and social data. It delivers data sets and grants data processing permits. It also conducts anonymization of personal data. Findata is authorized to grant permits for secondary use pursuant to the rules listed in chapter 5 of the Act.[64]

As to non-anonymized patient data, the Finnish Act on the Status and Rights of Patients (785/1992, as amended, in Finnish: *laki potilaan asemasta ja oikeuksista*) regulates the secrecy and confidentiality of the information contained in patient records. In addition, the Finnish Act on the Electronic Processing of Client Data in Healthcare and Social Welfare (159/2007, as amended, in Finnish: *laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä*) covers the electronic processing of personal data in social and health care.

The Medical Research Act (488/1999, as amended, in Finnish: *laki lääketieteellisestä tutkimuksesta*), enables access to personal data but includes a provision for data secrecy and confidentiality in chapter 5 section 28(2). It also covers very specific situations where limited disclosure of personal data is possible, for example an inspector must be given all requested documents that are necessary in an audit related to embryo research (chapter 5, section 22(2)).

In addition to the aforementioned, the list of applicable laws in the processing of social and health data is extensive. Further applicable rules can be found for example in

- GDPR
- The Finnish Data Protection Act
- Health Care Act 1326/2010
- Government Degree on patient documents 298/2009.

64. https://stm.fi/en/secondary-use-of-health-and-social-data (visited 15 February 2021).

this object represents a quantitatively substantial part of the general content of the protected database'.[7] If the obtaining, verification and presentation of specific simple data required very significant investment, the investment devoted to these data could be protected by a ban on the extraction of the simple data, which would protect these simple data by themselves. However, such a case remains very hypothetical, so that it does not seem really possible to protect simple data with an intellectual property right under French law.

Apart from the protection of data as themselves, data can be protected when integrated into databases.

Databases can be protected by copyright and by a *sui generis* right. Both protections can be cumulated. Such protection does not deal with data protection by itself but only with protection of the architecture of the databases, which is not the subject of this study.

c) Patent rights

Patents can be granted for any technical invention, as long as the invention is new, involves an inventive step and is industrially applicable.

An invention is patentable if it has a concrete and technical character, thus some inventions are not patentable because they are of an abstract and non-technical nature. Article L. 611-10 of the French Intellectual Property Code sets out these conditions, as well as a non-exhaustive list of what cannot constitute a patentable invention:

- Discoveries, scientific theories and mathematical methods;
- Aesthetic creations;
- Schemes, rules and methods in the exercise of intellectual activities, in the field of games or economic activities, or computer programs;
- Information presentations.

Unstructured data come from a primary source and have not been interpreted or subject to any processing or manipulation. Consequently, unstructured data is mere information, involves no inventive activity and cannot constitute a technical invention.

3. CONTROL OVER DATA BY CONTRACT INCLUDING BOUNDARIES FOR CONTRACTUAL RULES

Article 1112-2 of the Civil Code provides that: 'Anyone who uses or discloses confidential information obtained during negotiations without authorization is liable under the conditions of ordinary law.' In order to ensure data protection, however, it may be necessary to specifically include 'data' in the definition of confidential information.

It is necessary to provide for a definition of confidential information and a confidentiality clause at the contract execution stage. The definition must specifically include 'data' in order to ensure the protection of raw data. In the clause, the scope of the obligation and the exceptions should be specified).

7. CJEU 9 November 2004, C-203/02, *The British Horseracing Board Ltd and others*.

Article 1230 of the Civil Code provides that the confidentiality clause shall continue to apply after the termination of the contract. Article 1224 of the Code specifies that the resolution results either from the application of a termination clause, or from a notification or court decision in the event of sufficiently serious non-performance. In the absence of precision in the provisions of the Civil Code, it is necessary to provide that the confidentiality clause shall continue to apply for a fixed period after the end of the contract. It is also possible to provide for the restitution or destruction of the data.

A company or other legitimate holder may disclose its trade secrets and authorize their use to a third party under contractual conditions allowing them to maintain control of them (prohibition of disclosure, restrictions on use). This type of contract may provide for a ban on use after its expiry (post-term ban).

However, property is vulnerable as it depends on compliance with confidentiality obligations.

4. OTHER FORMS OF LEGAL PROTECTION CONTROLLING ACCESS TO, AND USE AND DISSEMINATION OF UNSTRUCTURED DATA

Data are subject to several protections, namely: trade secret, unfair competition, parasitism and criminal law.

a) Trade Secret

Trade secrets are protected by the provisions of Law No. 8218-670 of 30 July 2018 transposing Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. This Directive harmonizes protection for Member States, as many of them did not previously have protection.

The Law has been codified in Articles L. 151-1 et seq. of the Commercial Code.

To benefit from protection for trade secrets, the information must meet three conditions (Article L. 151-1 of the Commercial Code):

- It is not, in itself or in the exact configuration and assembly of its elements, generally known or easily accessible to people familiar with this type of information in their sector of activity;
- It has a commercial value, actual or potential, because of its secret nature;
- On the part of its legitimate holder (Articles L. 151-2 and L.151-3 of the Commercial Code), it is subject to reasonable protection measures, taking into account the circumstances, to keep it secret. In the event of a breach of a trade secret, the holder of the information must act within five years of the commission of the act which gave rise to the breach (Article L. 152-2 of the Commercial Code).

Only the legitimate holder can protect himself against a breach of trade secret, i.e. the person who lawfully obtained the information by one of the following two means:

- By an independent discovery or creation; or

- By observing, studying, disassembling or testing a product or an object which has been made available to the public or which is lawfully in the possession of the person obtaining the information, except if there is a contractual stipulation prohibiting or limiting the obtaining of secrecy (Articles L. 151-2 and L.151-3 of the Commercial Code).

The legitimate holder may be one to whom the information has been communicated under contract.

Acquiring a trade secret is illegal when it is done without the consent of the trade secret's legitimate holder and results from:

- Unauthorized access to any document, object, material, substance or digital file which contains the secret or from which it can be deduced, or from an unauthorized appropriation or copy of these elements;
- Any other behaviour considered, given the circumstances, to be unfair and contrary to commercial practice (Article L151-4 of the Commercial Code).

A company that is the victim of a violation of this secrecy can sue and claim:

- Provisional and conservatory measures to prevent or put an end to an infringement of a trade secret (Article L. 152-3-1 of the Commercial Code);
- Compensation for the damage suffered, taking into account the economic consequences (loss and loss of profit), the moral damage and the profits made by the infringer as well as the savings in investments (Article L. 152-6 of the Commercial Code);
- Publicity for the conviction decision (Article L. 152-7 of the Commercial Code);
- Payment of compensation (Article L. 152-5 of the Commercial Code).

b) Unfair Competition

This concept brings together a set of civil offences contravening commercial practice and sanctioned by extra-contractual liability under common law (Articles 1240 and 1241 of the Civil Code).

An action for unfair competition requires the demonstration of fault, damage and a causal link. The damage consists of a loss of customers or turnover, or even damage to the image, therefore the parties to the dispute must be in a competitive situation. The fault results from the risk of confusion with a competing company, acts conducting to a disorganization/disruption of a company, acts of disparagement or prohibited or unfair commercial practices disrupting the market. The damage is more often deduced from the existence of the fault constituting unfair competition.

The following crimes may be data breaches:

- Customer acquisition: the situation where a company creates confusion by imitating signs (brand, business name, reason or company name, domain name, brand, etc.) or products of a competitor to rally customers.
- The disorganization/disruption of the competing company by the use of technical knowledge or know-how (apart from disclosures by the director or

an employee of the victim company), either acquired via a former employee or during talks.
- The wrongful hiring of personnel with a view to diverting customers from a company by exploiting the knowledge acquired by the employee in his previous job.
- Creation of a competing company by former employees coupled with the exploitation of the knowledge and know-how of their former employer.

The instigator of the unfair competition action is the company that suffered the damage(s), in particular one that made the investments in the data. It may request compensation for its damage, the cessation of any actions possibly under penalty, seizures, as well as publication of the decision.

c) Parasitism

A parasitism action is also based on Article 1240 of the Civil Code which allows the engaging of the responsibility of an economic agent who interferes in the wake of another in order to profit, from its efforts and know-how.

Data have economic value. Their reproduction could therefore be penalized for parasitism, provided that the conditions discussed below are met.

Unlike unfair competition, parasitism does not require proof of a competitive situation between the parties to the dispute, nor of the existence of the likelihood of confusion. An action in parasitism supposes the demonstration of:

- the existence of investment,
- the non-accidental reproduction of the essential characteristics of the service or product,
- the realization of profits drawn from the elements taken back.

Parasitism can embrace a wide range of situations fulfilling the conditions mentioned above. For example, the capture of research and development investments is sanctioned under parasitism. The Court of Cassation held that the use of specific know-how, without investing in its development, constitutes an act of parasitism.[8] In particular, it was held that the reproduction of statistical studies was judged parasitic in that 'even if they are not protected by a specific private right, statistical studies are the result of a know-how in the conception methods of polls, important services for the execution of these and intellectual work for their exploitation. By publishing such data without the slightest consideration, a press organ appropriates what could only be obtained through the work of others and commits an act of parasitic competition'.[9]

In the area of parasitism, the applicant bringing the action must demonstrate that he has spent significant human and/or financial resources to constitute and/or operate the database. In reality, this action is based on Article 1240 of the Civil Code, which constitutes, to a certain extent, a parallel regime to that of the *sui generis* regime of the Intellectual Property Code, from which the producers of databases

8. Com. 10 September 2013 No. 12-20933.
9. CA Paris, 22 May 1990: D . 1990, inf. Rap. p. 175.

iii) Breach of Trust

Article 314-1 of the Penal Code provides that: 'Breach of trust is the act by a person of misappropriating, to the detriment of others, funds, securities or any property that has been handed over to him and that was accepted on condition of returning them, representing them or making a specific use of them'.

Breach of trust requires the following constituent elements:

- provisional delivery based on an agreement, the law or a judicial decision of funds/securities/goods,
- an act of embezzlement: this is not defined by the Penal Code, but case law has specified that the embezzlement does not require that the accused has appropriated the thing entrusted to himself, nor that he derived a personal benefit from it, it suffices that the owner can no longer exercise his rights over it.'

Breach of trust is an intentional offence, which implies that the perpetrator must have wanted to misappropriate the property and was aware of the provisional nature of his holding of the fund/security/property.

The Court of Cassation held that an employee 'who knowingly misappropriated computer files containing confidential information and made available for professional use by duplicating them for his personal use, to the detriment of his employer' constituted a breach of trust.[15]

Breach of trust is punishable by three years' imprisonment and a fine of EUR 375,000. The penalty is increased to seven years' imprisonment and a fine of EUR 75,000 if the offence is committed by an organized gang or if the breach of trust is carried out to the detriment of a person whose particular vulnerability is apparent or known to the perpetrator.

iv) Extortion

Article 312-1 of the Penal Code provides that: 'Extortion is the act of obtaining by violence, threat of violence or coercion either a signature, an undertaking or a waiver, or the revelation of a secret, or the delivery of funds, securities or any property.'

The material element of extortion is characterized by:

- the means of extortion: violence, threat of violence or coercion,
- the result of the extortion: obtaining a signature, a commitment, a waiver, the revelation of a secret, or the delivery of funds, securities or any property.

Extortion is an intentional offence, meaning that the perpetrator must have desired the outcome of the offence. For some authors, this offence could be applied in the case of crypto-locking (a cyberattack carried out using software to encrypt data and thus forcing the victim to pay a ransom).

Extortion is punished by seven years' imprisonment and a fine of EUR 100,000. It is punishable by ten years' imprisonment and a fine of EUR 150,000 if it is preceded,

15. Crim. 22 October 2014 No. 13-82630

accompanied or followed by violence or committed to the prejudice of a person whose particular vulnerability is apparent or known to its perpetrator. Extortion committed by an organized gang is punishable by twenty years' imprisonment and a fine of EUR 150,000.

v) Blackmail

Article 312-10 of the Penal Code provides that: 'Blackmail is the act of obtaining, by threatening to reveal or impute facts liable to damage the honour or reputation, a signature, a commitment or a waiver, resulting in the revelation of a secret, or the delivery of funds, securities or any good'.

The means used to obtain the return of funds/valuables/goods may vary, it is a threat of an attack on honour or reputation, which requires a demonstration of the defamatory nature of the revelation or imputation.

The result of blackmail is similar to that of extortion, in that it involves obtaining a signature, an undertaking or a waiver, and the revelation of a secret, or the delivery of funds, securities or any good.

Blackmail is an intentional offence which requires that the perpetrator has used this specific threat knowingly and in order to obtain the property/value claimed. For some authors, this offence could be applied in the cases of ransomware (malicious software which prevents access to data stored on a computer and only provides access on payment of a ransom). Blackmail is punished by five years' imprisonment and a fine of EUR 75,000. If the perpetrator has carried out his threat, the sentence is increased to seven years' imprisonment and a fine of EUR 100,000.

vi) Breach of Automated Data Processing Systems (STAD)

An infringement can result from two types of offence:

- fraudulently introducing data into an automated processing system, and extracting, holding, reproducing, transmitting, deleting or fraudulently modifying the data it contains;[16]
- without a legitimate reason, in particular for research or computer security, to import, hold, offer, transfer or make available equipment, an instrument, a computer program or any data designed or specially adapted to commit one or more of the offences provided for in Articles 323-1 to 323-3.[17]

Infringements of STAD are punishable by penalties ranging from two to five years' imprisonment and a fine of EUR 60,000 to 150,000.

e) Breaches of Trade Secrets

Article L. 621-1 of the Intellectual Property Code, referring to Article L. 1227-1 of the Labour Code, criminalizes infringement of trade secrets. Article L. 1227-1 of

16. Article 323-3 of the Criminal Code.
17. Article 323-3-1 of the Criminal Code.

applicable to incorporeal products.[74] The protection against imitation under Section 4 No. 3 of the German Unfair Competition Act protects against unfair imitations of a product or service. Whether this can be applied to data has not yet been clarified. If this were the case, data would have to have a distinctive character under competition law, which is unlikely to be the case as a rule.[75] German competition law thus offers at best weak legal protection of data that is limited to certain constellations, and this protection is fraught with legal ambiguities.

c) Tort Law

Section 823 (1) of the German Civil Code is a general clause of tort law. According to Section 823 (1) German Civil Code, 'anyone who intentionally or negligently causes unlawful injury to the life, limb, health, freedom, property or other right of another' is liable to pay damages. According to the general reading, the recognition of a legal position as an 'other right' within the meaning of Section 823 (1) German Civil Code presupposes that this right can be qualified as an absolute subjective right.[76] This in turn presupposes that the right assigns an allocation or use function and an exclusion function to the position.

The general clause of Section 823 German Civil Code has often been adapted to technical changes; for example, domain names, the right of personality, or expectant rights are now subsumed under 'other rights'.

Another approach is therefore to regard a right to data as a new 'other right' within the meaning of Section 823 (1) German Civil Code.[77] However, the basis and scope of such protection are disputed. For example, the Supreme Court has classified data as an 'independent asset'.[78] In part, the protection of data is compared with the protection of property,[79] which is protected as an 'other right', in part this is said to be justified by the general lack of protection of data compared to physical objects. This right is intended to guarantee the person who stores the data integrity protection of the data, which exists independently of the ownership of the data medium and in any case includes the deletion or modification of data. In order to limit the protection, it is proposed to restrict it, in line with the restriction in database producer protection,

74. Still on Sec. 4 No. 9 UWG: Helmut Köhler, *Gesetz gegen den unlauteren Wettbewerb* (C.H. Beck, 2021) Sec. 4 para. 9, 22.
75. *See also* Herbert Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers"' *CR* (2015) pp. 137, 143.
76. Reichsgericht für Zivilsachen, judgment of 29 February 1904 – VI. 311/03, *RGZ* 57 pp. 353, 356 et seq.
77. Herbert Zech, 'Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers"' *CR* (2015) pp. 137, 143; Spindler, *Bürgerliches Gesetzbuch* (BeckOK, 2021) Sec. 823 para. 93; Helmut Redeker, 'Information als eigenständiges Rechtsgut', *CR* (2011) pp. 634 et seq.; Andreas Wehlau/Klaus Meier, 'Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung', *NJW* (1998) pp. 1585, 1588 et seq.
78. Supreme Court, judgment of 2 July 1996 – X ZR 64/94, *NJW* (1996) pp. 2924, 2926.
79. *Cf.* Helmut Redeker, 'Information als eigenständiges Rechtsgut', *CR* (2011) pp. 634, 638 et seq.

to data collections of significant importance that are characterized by significant disadvantages in the event of infringement.[80]

The right of individuals to use their own data and to prevent third parties from unauthorized use or interference with their data derives from the right to privacy and says nothing about non-personal data.

Protection under Section 823 (2) of the German Civil Code is also discussed in this respect. Under Section 823 (2) German Civil Code, a person who violates a law intended to protect another person is liable for damages. Such protective laws within the meaning of Section 823 (2) German Civil Code are the criminal provisions of Section 303a and Section 202a of the German Criminal Code. However, Section 303a German Criminal Code only protects against data being altered, while Section 202a German Criminal Code protects against data being deleted or damaged, and neither standard therefore protects against any other (unauthorized) use. This means that a duplication or other use, for example in the context of an analysis of the stored data, is not seen as a violation of such a right.[81] It also follows that a miscellaneous right to data under Section 823 German Civil Code does not provide protection against access by third parties in the sense of an exclusive right.[82] Neither an economic assignment content nor a transferable legal position result from the recognition as a tort protected position.[83]

The fundamental right to confidentiality and integrity of information technology systems recognized by the Federal Constitutional Court[84] is also intended to serve as the basis for the other right to data under Section 823 German Civil Code.[85] According to this, economic use without impairing the integrity of the data could also constitute an infringement. However, since the fundamental right to confidentiality and integrity of information technology systems is based on the protection of personality, the information technology system would have to be relevant to personality, which is not the case with pure machine-to-machine communication and the resulting data.[86]

If all this is taken together, a mere anchoring of a property right to data via the construction of other rights in Section 823 (1) German Civil Code seems rather daring, especially since the analogy to the right of personality, which is also protected via Section 823 (1) German Civil Code, is weak, since in the case of the latter there was a constitutional justification at the beginning, which was then only transferred to civil law.

80. Michael Bartsch, *Recht der Daten und Datenbanken im Unternehmen* (Otto Schmidt, 2014) pp. 297, 301 et seq.
81. Ansgar Ohly, *Digitale Daten in Geräten und Systemen* (Carl-Heymanns, 2010) pp. 123, 135.
82. Thomas Thalhofer, 'Recht an Daten in der Smart Factory', *GRUR-Prax* (2017) pp. 225, 226; Louisa Specht, 'Ausschließlichkeitsrechte an Daten – Notwendigkeit, Schutzumfang, Alternativen', *CR* (2016) pp. 288, 289.
83. Herbert Zech, 'Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt', *GRUR* (2015) pp. 1151, 1158.
84. Supreme Court, judgment of 27 February 2008 – 1 BvR 370/07, 1 BvR 595/07, *NJW* (2008) p. 822.
85. Michael Bartsch, 'Die „Vertraulichkeit und Integrität informationstechnischer Systeme" als sonstiges Recht nach § 823 Abs. 1 BGB', *CR* (2008) pp. 613, 614 et seq.
86. Herbert Zech, 'Industrie 4.0 – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnenmarkt', *GRUR* (2015) pp. 1151, 1158.

the national level, the re-use of public sector information is covered by the PSI/Open Data Directive 2019/1024 of 20 June 2019 PSI Directives 2003/98/EC and 2013/37/EU.

The existing German Act on Re-use of Public Sector Information (IWG) has to be amended by 17 July 2021. Public sector information legislation establishes a subjective right that documents (content) in the public sector should be provided for re-use in the private sector without discrimination and at fees equating marginal costs. Documents should be open access by design and default. Licences should be open access and provide limited discretion to include restrictions. Exceptions include protection of intellectual property rights, trade secrets and data protection law. Publicly funded research data would be included. The obligations are also extended to public undertakings unless in direct competition with private companies. Articles 13, 14 Open Data Directive also introduced a new category of 'high value data sets' relating to special thematic areas (geo, statistics, mobility etc.) and their potential to generate significant socioeconomic or environmental benefits and innovative services; benefit SME's and be combined with other data sets. These data sets should be provided freely via APIs. This obligation comes close to an obligation to proactively publish public sector information that is included in different German legislation on a federal level (Section 12a EGovG) as well as state level (e.g., Section 11 (4) BremIFG, Section 3 HmbTG), the latter mostly applying to limited catalogues of information. This seems to be the way to go ahead. A proactive obligation to publish public sector information on the internet could merge rights of access with rights of re-use in one integrative approach.

Access to public sector information is left to the Member States of the European Union, with the exception of documents of European institutions (FOI Regulation 1049/2001) and geodata (INSPIRE Directive 2007/2/EC). In Germany, access is regulated in the Freedom of Information Act for the federal administration and by state laws for most of the states. Access to official information will be granted without any special requirements. This also includes documents provided to the administration by third parties. Access may be denied for different reasons, including intellectual property, trade secrets and data protection, but with a slightly different scope than applied to the re-use. For example, intellectual property rights would prevent access if access would lead to an infringement whereas re-use would be already excluded if IP rights exist. Sometimes administrations claim a disproportionate administrative burden as an excuse which is not included in the statutes, however. The public bodies are requested not to exercise their own intellectual property digital rights. The re-use of information is a way to add value to the data that may be benefitting the public sector when looking at data flow as a circle in a connected environment. This increasingly blurs the boundary between public sector information and privately held information.

In Germany, following French legislation[93] and sparked by the EU Commission[94] an intense debate has been going on to create access rights to privately

93. Loi No. 2016-1325 of 2016, JO République Francaise No. 0235 of 2017.
94. Commission Staff Working Document on the free flow of data and emerging issues of the European data economy, *SWD* (2017) 2 final of 10 January 2017, pp. 36 et seq., available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0002&from=EN (accessed 24 March 2021).

held information with respect to certain types of data (public interest data) or specific sectors with high relevancy of data sharing. Access rights could be rooted in compulsory licensing concepts from cartel law, but the regulatory framework would go beyond that. The rights could be granted to private companies as well as public bodies. In its European Data Strategy[95] the EU Commission announced the promotion of data sharing in the business-to-government (B2G) sector as well as the business-to-business sector and plans to adapt the framework of intellectual property in machine data. Moreover, the plan is to create 'Common European Data Spaces' for certain sectors (industrial, green mobility, health, financial, energy, agricultural, public procurement). This should promote the availability of data in these sectors, combined with the technical tools and infrastructures necessary to use and exchange the data, as well as appropriate governance mechanisms. The horizontal framework should be complemented by sectoral legislation for data access and use, and mechanisms for ensuring interoperability.

b) Health Data

In Germany there is currently no legislation on non-personal data in the health sector. This is probably because under German law it is as yet unclear which data in the health sector can be non-personal at all, since health data can nearly always be traced back to an identifiable person. It would be conceivable that the personal reference could be removed by anonymizing the corresponding data. The legal basis for such anonymization and the consequences for the anonymized and thus non-personal data obtained in this way are currently under discussion in Germany. It is also unclear which technical standards are to be used as a basis for achieving the necessary validity of the anonymization process.

In line with the above, there are as yet no specific legal regulations in Germany on access to non-personal data in the health sector. However, German regulations regarding the processing of personal data within health and medical care can be found in the Patient Data Protection Act (PDSG), which entered into force in October 2020. It provides for voluntary data release of the patient for medical scientific research (so-called data donation) as well as the regulation of access to patient data for corresponding medical and nursing institutions and service providers. In addition, Regulation (EU) 2017/745 (Medical Devices Regulation) stipulates in Article 10 para. 14 a right of access for corresponding authorities to all information necessary to check the conformity of a medical device. This may also include data.

95. A European strategy for data, *COM* (2020) 66 of 19 February 2020, available at: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf (accessed 24 March 2021).