Q274 IP rights in data – answers of the Dutch Group

Participants working Group: Martin Hemmer – chairman (AKD), Benjamin Niemeijer (La Gro Geelkerken), Bertrand ter Woort (De Brauw Blackstone Westbroek), Douwe Linders (SOLV advocaten), Peter van Schijndel (Hoyng Rokh Monegier)

I. Current law and practice

Please answer all questions in Part I on the basis of your Group's current law.

A. Protection of mere data

For the answers to this question, the definition of "data" and "mere data" is crucial.

The original definition, in paragraph 15 of the questionnaire, was as follows.: *"'Data" means any mere information (individual item) of any kind, not aggregated and not arranged in a systematic or methodical way.*

The committee later issued guidance on how to interpret this definition:

> *"The intent of the definition is to distinguish between unstructured data, i.e., data that may be aggregated but is not structured, and structured data, i.e., data that has been aggregated AND stored in a systematic or methodical way in a database.*
>
> *Consequently, the definition of "mere data" should be understood as: "any mere information (individual item) of any kind, not structured and not arranged in a systematic or methodical way, that is recorded and stored by electronic or other means".*

The **first**, slightly philosophical, point is to note that the definition apparently seeks to draw a distinction between data and information in general. Data is defined as being an individual unit of information. Such a definition appears to fall in line with scholarly frameworks for modelling the relations between data, information and knowledge (or even wisdom), such as the DKIW pyramid.[1] Oetinger[2] had the following to say about this:

> Data can be defined in a multitude of ways, very often depending on the sector one observes (Kocharov 2009, 336).[6] However, data at a fundamental level are defined by Ackoff as 'symbols that represent the properties of objects and events. Information consists of processed data, the processing directed at increasing its usefulness' (Ackoff 1999, 170–172). Therefore it is quite common that data are defined in their relation to information and knowledge. Another definition of data, including their relation to knowledge proposes that data are defined as uninterpreted symbols; information is data with added meaning; and knowledge is the ability to assign meaning to data in order to gain new information.[7] This trichotomy implies a hierarchy where data are the precursor of information, which is the precursor of knowledge. There is a linear flow between the concepts which also result in added value for the user and holder of the data. These considerations are not merely theoretical, as data in an economic and business context are sought precisely for the purpose of deriving further information and knowledge.

The data item "red", for instance, becomes useful information when it is contextualized as the color displayed by a traffic light at the intersection. The message conveyed by that information is that the (self-driving) car should stop. The mere data "red" does not provide that insight.

If such a distinction is indeed to be drawn in the questionnaire, then the consequence could be that a proposal to protect data does not also cover data which has become information. That could create a lacuna of protection (if protection is indeed desired).

Our **second** observation is that after the clarification by the committee, "data" now excludes structured data, with the qualification that this concerns the individual units of information. The Dutch group is afraid that this may have introduced a

[1] *https://en.wikipedia.org/wiki/DIKW_pyramid*

[2] *https://www.tandfonline.com/doi/full/10.1080/13600869.2019.1631621*

new unclarity. It would be perfectly clear and understandable if the committee wants to exclude structured **sets** of data (such as a database) from the scope. The definition however seems to suggest that it concerns not sets of data, but rather a distinction between "single units of information" which can be structured or which can be unstructured.

In that particular sense, we understand 'structured data' to be data (including “mere information”) that has a particular and fixed format. Three examples to help clarify:

- A sensor that measures temperature and records it in degrees Kelvin using the continental European standard for the decimal separator (a comma), produces structured data. At the time of writing this document, the temperature in Amsterdam was "288,75".

- A motion detector that records in a log the times when motion was detected, will generally also be outputting structured data: "20200506-17:45:16" for instance.

- Street addresses are structured data, with the structure differing from country to country. In the Netherlands, the common structure is "[Streetname] [number]". The French use "[number] [Streetname]".

Unstructured data, on the other hand, is data that has no fixed schema. An example would be customer reviews on a website. The content of such a review is free text, without an imposed structure. Photos can also be regarded as a form of unstructured data: the contents of the photo and its composition are generally chosen by the photographer.

The Dutch group sees no reason why structured data (as in a single unit of information) should fall outside the scope. Such a limitation would mean that a majority of the useful and valuable information to which the introduction of the questionnaire refers is not considered. The Dutch Group thus assumes that there was no intention to exclude structured data (individual unit of information), as opposed to structured sets of data (such as a database), from the scope of the review.

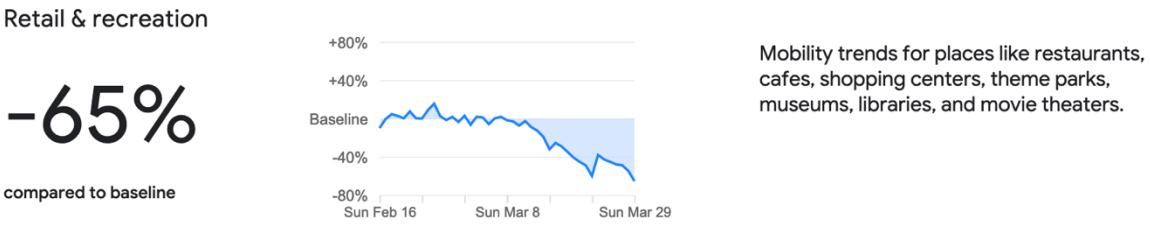
Third, and perhaps most importantly, the definition after clarification could be seen to imply that only data that is recorded is in scope: "*data […] that is recorded and stored by electronic or other means*". If that is how the definition is to be read, it would exclude data that is not recorded, but which is created on the basis of other data (which may, or may not, have itself been directly recorded). Take for instance the average, mean, median, or the sum of data points. The same applies to data that was anonymized or otherwise altered. Such derived data is not itself "recorded" by a sensor or observer and would fall outside the scope of the present definition.

Excluding data for the simple reason that it was not recorded directly does not seem logical, or desirable, from a point of economic value and relevance. A couple of examples to help explain

(i) Average measurements: a measurement with N=1 is generally unreliable. To get more reliable or meaningful data, sampling and averaging is often used. Weather data is a good example: a single reading can be off due to a passing cloud or a gust of wind. The average temperature, with a sufficiently high sampling rate, is more reliable. Sampling and averaging is also frequently used in automative and aerospace applications.

(ii) Summed data: The present COVID-19 crisis is a fitting example. In the past few months we have all been looking at graphs and exponential curves of summed up data. Number of new patients per day. Number of deaths. Number of recoveries. None of these data points was itself measured. There is no sensor or person that directly observed *"1015 new confirmed infections, today, in the Netherlands"*. Instead, it is the sum of all the separate reported cases. This summed up data has been of tremendous value, and has informed policies and measures worldwide. Yet would fall outside the scope of the present definition.

(iii) Anonymized data: In light of data protection and privacy laws, data is often anonymized by aggregation. An example from the Covid-19 response can help clarify. In shaping its policies and monitoring their effect, the Dutch government has relied on location data provided by Google that shows the mobility of the Dutch citizens. Google provided no individualizable data, but only aggregated and relative figures, c.f. the example below. These particular data items were (naturally) not recorded, but derived. The Dutch Group sees no reason why this type of data should be excluded from the definition.



In answering the below questions, we have assumed that the definitions set by the committee only seek to exclude structured data sets from the scope of this exercise but wishes to keep structured data (single units of information) and derived and (directly) created data in scope.

1) Can mere data (in general or some specific mere data) be subject to a property right / IP right? If yes, please answer the following sub-questions:

No: Mere data, as per the definitions, is not protected by any property / IP right in the Netherlands.

Obiter, it is noted that in 2012 the Dutch Supreme Court (ECLI:NL:HR:2012:BQ9251) held that under certain conditions digital items can be stolen. The case concerned the game Runescape, which allowed players to acquire, trade and lose in-game items. In the physical world, two players had physically assaulted a third player and forced him to login to Runescape after which they proceeded to rob him of his in-game possessions. After this altercation in the physical world, the in-game items (a digital mask and a digital amulet) were no longer in the digital inventory of the victim.

The Supreme Court ruled that given the circumstances of the case, the mask and amulet were to be classified as a "good" and not simply as "data". A key consideration was that given the rules of the game Runescape, the mask and amulet had unicity: they could only be in the possession of one account. The Supreme Court held that the Court of Appeal was right to consider that *"[…] the victim had within the confines of the game the 'factual and exclusive possession' over the amulet and mask and has through the acts of the perpetrators lost possession of these objects".*

The Dutch Group considers that such circumstances will not generally arise in respect of the mere data to which the present questionnaire is directed. By their very nature, data can be copied and multiplied without the original being lost or removed from the possession of the original holder. Barring a context or system in which unicity is imposed on mere data, they are unlikely to be considered a good in the way that the Runescape mask and amulet were.

a) **What type of property right / IP right would this be?**

b) **What are the requirements for such protection?**

c) **Who is the owner of this property right?**

d) **What acts are prohibited for third parties to avoid infringement?**

e) **Is this right marketable? If so, are specific rules in contract law applicable?**

f) **Does your legislation/case law contain specific exceptions to this protection (*e.g.* access right for data mining, scientific research, etc.)?**

2) Is mere data protected by provisions other than a property right / IP right? If yes, please answer the following sub-questions:

a) What type of protection is available?

Mere data could be protected by EU Trade Secrets Directive which is implemented in the Netherlands under the Trade Secrets Act (*Wet bescherming bedrijfgeheimen*).

The definition of trade secrets is flexible enough to also cover data whose commercial value only arises from the possibility to discover valuable information through the means of big data analytics. [3]

b) What are the requirements for such protection?

There are three cumulative requirements for protection,

1. it 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;

2. it has commercial value because it is secret; [4]

3. it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

c) Who is the person entitled ?

Holder of the trade secret can claim the enforcement remedies under the Trade Secrets Act in case of a violation. Article 1 Trade Secrets Act defines the holder of the trade secret 'as the natural or legal person controlling the trade secret'.

Note that the holder of the trade secrets does not 'own' the underlying information.

d) What acts are prohibited for third parties to avoid infringement?

The acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful, whenever carried out by:

(a)unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;

(b) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions:

(a) having acquired the trade secret unlawfully;

(b) being in breach of a confidentiality agreement or any other duty not to disclose the trade secret;

(c) being in breach of a contractual or any other duty to limit the use of the trade secret.

The acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

[3] http://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf

[4] *Recital 14 Trade Secrets Directive only gives an indication on what is harm-based. The directive is silent on the quantitative threshold of the commercial value.*

The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully

e) Are mere data marketable? If so, are specific rules in contract law applicable?

Under Dutch contract law mere data is marketable in such a way that parties agree by way of contract to secrecy and/or access rights to the data.

There are no specific rules in contract law that consider mere data.

f) Does your legislation/case law contain specific exceptions to this protection (*e.g.* access right for data mining, scientist research, etc.)?

Other than EU Directive 2019/790 of 17 April 2019 on copyright and related rights in the Digital Single Market, that provide an exception to copyright for text and data mining for the purposes of scientific research (Article 3 and 4) there is no specific legislation / case law.

B. Protection of databases

3) Can a database be subject to a property right / IP right? If yes, please answer the following sub-questions:

Yes

a) What type of property right / IP right would this be?

Both a *sui generis* database right and copyright. The European Directive 96/9/EC of 11 March 1996 on the legal protection of databases ("Database Directive") is implemented into the Dutch Database Act, which contains the sui generis right, and an amendment to the Dutch Copyright Act. Both the Copyright Act and the Database Act offer protection to databases.

b) What are the requirements for such protection?

Protection of databases under the Dutch Copyright Act:

Article 10(3) of the Copyright Act stipulates that compilations can be protected by copyright:

"Collections of works, data or other independent materials arranged in a systematic or methodical way and individually accessible by electronic or other means, shall be protected as separate works, without prejudice to other rights in the collection and without prejudice to copyright or other rights in the works, data or other materials incorporated in the collection."

The criterion for protection is that of article 3(1) of the Database Directive. A database is protected by copyright if the database "by reason of the selection or arrangement of its contents, constitutes the author's own intellectual creation." The criterion has been interpreted by the European Court of Justice ("ECJ") in its 2012 judgment in *Football Dataco/Yahoo*. According to the ECJ a database within the meaning of Article 1(2) of the Database Directive is protected by copyright provided that "the selection or arrangement of the data which it contains amounts to an original expression of the creative freedom of its author."[1] As a consequence:

- "the intellectual effort and skill of creating that data are not relevant in order to assess the eligibility of that database for protection by that right;
- it is irrelevant, for that purpose, whether or not the selection or arrangement of that data includes the addition of important significance to that data; and
- the significant labour and skill required for setting up that database cannot as such justify such a protection if they do not express any originality in the selection or arrangement of the data which that database contains." [2]

In general, the level of originality required by Dutch courts is very casuistic but tends to be rather low.

Based on *Football Dataco/Yahoo* , the Dutch Supreme Court ruled in 2014 that the protection of non-original compilations (as "impersonal works") in the Dutch Copyright Act was contrary to the maximum harmonization in the Database Directive.[4] Protection of impersonal works was removed from the Dutch Copyright Act on 1 January 2015.

Registration is not required for protection.

[1] ECJ 1 March 2012, case C-604/10 (*Football Dataco/Yahoo*), paragraph 45.

[2] ECJ 1 March 2012, case C-604/10 (*Football Dataco/Yahoo*), paragraph 46.

[3] ECJ 1 March 2012, case C-604/10 (*Football Dataco/Yahoo*), paragraph 52.

[4] Dutch Supreme Court 17 January 2014, ECLI:NL:HR2014:88 (*Ryanair/PR Aviation*).

Protection of databases under the Dutch Database Act:

Pursuant to Article 1(1)(a) of the Dutch Database Act a collection of data must meet the following requirements in order to be protected by database law:

1. It is a collection of works, data or other independent elements;
2. The works, data or elements are systematically or methodically organized;
3. The works, data or elements are accessible separately by electronic means or otherwise; and
4. The obtaining, verification or the presentation of the contents of the database testifies, qualitatively or quantitatively, to a substantial investment.

Re (i) A collection of works, data or other independent elements

The requirement that a collection consists of "independent elements" means that it should concern elements that can be separated from each other without affecting their independent informative content. The independent informative value of an element extracted from a collection should be assessed in light of the value that the information has for any third party interested in that element, and not in the light of the value that this information has for a typical user of the collection. A stand-alone element may also exist in a combination of data.[1]

Re (ii) Systematically or methodically ordered

Requirement (ii) aims to exclude unorganized information from the definition. However, if elements are not organized, the use of other means, such as a search engine, may turn a collection of unorganized data into a protected database.

Re (iii) Separately accessible

Requirement (iii) is fulfilled when the different parts of the database can be retrieved individually.[2] The (digital) database must be searchable in its entirety. The ECJ emphasizes that there must be a 'means' to retrieve each of the elements making up the database.[3]

Re (iv) Substantial investment

Discussions on the applicability of database law to a data collection usually focus on the requirement under (iv) of a substantial investment. It is this investment that forms the basis for database protection. The investment may consist of money, but also, for example, of time and effort put into the database. The substantial investment must relate to the obtaining, verification or the presentation of the contents of the database.

The concept of 'investment in obtaining the content' means that the investment must relate to the means used to obtain existing elements and to collect them in a database, and not to the means used to create those elements.[4] In the *British Horseracing* case*, for* example, the question was whether an organiser of horseraces was entitled to database protection on race schedules. The Court ruled that, for example, the investments relating to the determination of the horses that were allowed to participate could not be taken into account in the assessment of the substantial investment, since those investments related to the creation of the elements making up the content of the database.

The term 'investment in verifying the contents' of the database refers to the investment made in verifying the accuracy and completeness of the contents of the database, both at the time it is set up and during its operation, in order to ensure the reliability of the information contained in the database.[5]

The term 'investment in the presentation of the contents' of the database refers to investments made with a view to the systematic or methodical arrangement of the elements and the organization of their individual accessibility, but also to investments in, for example, the user interface and the layout of the database, i.e. its visible exterior.[6]

[1] CJEU 29 October 2015, Case C-490/14 (*Freistaat Bayern v Verlag Esterbauer*), paragraphs 17, 20, 22, 23 and 27, referred to by the Dutch Supreme Court in its judgement of 8 June 2018, ECLI:NL:HR:2018:856 (*Pearson/Bär*).

[2] *Explanatory Memorandum to the Database Act,* 1998/99, 26108, No 3, p. 8.

[3] ECJ 9 November 2004, case C-444/02 (*Fixtures/OPAP*).

[4] ECJ 9 November 2004, Case C-203/02 *(British Horseracing Board/William Hill)* and ECJ 9 November 2004, Case C-444/02 *(Fixtures Marketing/OPAP)* paragraph 40.

[5] ECJ 9 November 2004, Case C-203/02 *The British Horseracing Board/William Hill,* paragraph 34.

[6] CJEU 9 November 2004, Case C-444/02, (*Fixtures Marketing/OPAP*), paragraph 34 and District Court of The Hague 22 February 2009, *Media Forum* 2009/10 (*Autotrack/Gaspedaal*).

c) Who is the owner of this property right?

Owner of databases under the Dutch Copyright Act:

Pursuant to article 1 of the Copyright Act, the author of an original compilation is the owner of the exclusive rights thereto. In case of a compilation of various copyrighted works, the compiler is explicitly considered the author of the compilation as a whole (article 5(1) of the Dutch Copyright Act). Where labour which is carried out in the service of an employer consists in the making of certain works, the employer is considered the author (article 7 of the Dutch Copyright Act). A public institution, an association, a foundation or a company that communicates a work to public as its own, without naming any natural person, is considered to be the author, unless it is proven that the communication was unlawful (article 8 of the Dutch Copyright Act).

Under the Dutch Copyright Act, copyright passes by succession and is transferable by assignment in whole or in part (article 2(1) of the Dutch Copyright Act). In addition, the owner may grant a license for all or part of the copyright (article 2(2) of the Dutch Copyright Act).

Owner of databases under the Dutch Database Act:

The rights laid down in article 2 of the Database Act are granted to the “producer” of the database. The database “maker” does not own any rights. Pursuant to article 1(1)(b) of the Dutch Database Act, the producer is the person/organization bearing the risk for the investment in the database. The Dutch legislator has explained that this means that not the factual manufacturer of a database is the owner, but the customer ordering the database, if this customer is the one bearing the risk.[1] It is argued amongst Dutch legal scholars that this definition lays too much emphasis on the financial investment criterion.[2]

[1] *Explanatory Memorandum to the Database Act,* 1998/99, 26108, No 3, p. 2.

[2] See J.H. Spoor, D.W.F. Verkade & D.J.G. Visser, *Auteursrecht*, Deventer: Kluwer 2019, p. 809.

d) What acts are prohibited for third parties to avoid infringement?

Protection of databases under the Dutch Copyright Act:

Third parties are prohibited from communicating a copyright protected compilation to the public, including the making available of the compilation to the public, from distributing copies of the compilation to the public (article 12 of the Dutch Copyright Act

and article 3 and 4 of the InfoSoc Directive (2001/29)), and from reproducing a compilation (article 13 of the Dutch Copyright Act and article 2 of the InfoSoc Directive), subject to the limitations laid down by law.

Protection of databases under the Dutch Database Act:

Extraction is the temporary or permanent transfer of the content of all or part of a database to another carrier (Article 1(1)(c) of the Database Act). It is not necessary that there is actual technical 'copying'. Also, for example, copying a database by hand may be considered an extraction.[1]

Re-utilization is making available to the public the content of all or part of a database, in any form, by means of distribution of copies, rental, on-line transmission or transmission in another manner (Article 1(1)(d) of the Database Act). The offering or provision of a dedicated search engine that can search a database may also fall within the scope of re- utilization under certain circumstances.[2]

The extraction or re-utilization of a “substantial part” can be understood both qualitatively as quantitatively. This shows that it is not so much the quantity of data that is relevant, but its commercial value. According to the explanatory memorandum to the Dutch Database Act, a “substantial part” is deemed to have been extracted if such a part is extracted that the user thereby benefits substantially from the commercial value of the database or causes substantial damage to the database producer.[3]

Quantitatively' refers to the amount of data extracted or re-utilized in relation to the total size of the database. Qualitatively' refers to the size of the investment made in the obtaining, verification or presentation of the specific part of the database which is extracted or re-utilized, even if that part is negligible in quantitative terms.[4] From a human, technical or financial point of view, even such a part may represent a substantial investment. It should be noted that the intrinsic economic value of the individual elements of the database is irrelevant. For example, a current share price may have a high economic value, that does not mean that it is a qualitatively substantial part of the database.[5]

The acquisition of a qualitatively or quantitatively non-substantial part may also infringe a database right. This is the case if non-substantial parts of the contents of the database are repeatedly and systematically extracted or re-utilized. Such repeated and systematic extraction or re-utilization must be contrary to the normal exploitation of the database or cause unjustified damage to the legitimate interests of the producer of the database. The decisive factor here is whether the database is, as it were, reconstructed (to a substantial extent).[6] The producer of the database is then in danger of losing exploitation proceeds. This deprives the producer of income which can cover the costs of his investment in the database.[7] Repeated and systematic extraction or re-utilization of non-substantial parts which are then immediately erased, are not covered by this criterion.[8] In that case, there is no cumulative effect and it does not reconstruct all or a substantial part of the contents of the database.

[1] ECJ 9 October 2008, case C-304/07 (*Directmedia/University of Freiburg*).

[2] ECJ 19 December 2013, case C-202/12 (*Autotrack/Gas pedal*).

[3] *Explanatory Memorandum II* 1997-1998, 26108, No 3, p. 10.

[4] ECJ 9 November 2004, C-203/02 (*BHB/ William Hill)* paragraphs 71 and 72.

[5] J.H. Spoor, D.W.F. Verkade, D.J.G. Visser, *Copyright, neighbouring rights and database right*, Deventer: Kluwer 2019, p. 817.

[6] ECJ 9 November 2004, C-203/02 (*BHB/ William Hill)* paragraph 87.

[7] ECJ 19 December 2013, C 202/12 (*Autotrack/Gaspedaal)* paragraph 41.

[8] ECJ 9 November 2004, C-203/02 (*BHB/ William Hill)* paragraphs 90 to 94.

Note that the producer of a database cannot prohibit, on the basis of his sui generis right, the manufacture of a similar database by a third party who does not use data from the producer’s database, since in that case no extraction or re-utilization would be involved. The producer may have cause of action based on copyright.

In addition, Article 5a of the Database Act provides that the person who bypasses effective technical provisions and who knows or can reasonably be expected to know this is acting unlawfully. Furthermore, Article 5b Database Act prohibits the

removal or modification of electronic information concerning the management of rights and the distribution, entry, etc. of databases that have been removed or modified in an unauthorized manner. This provision applies only to electronic information.

e) Does your legislation/case law contain specific exceptions to this protection (*e.g.* access right for data mining, scientist research, etc.)?

Protection of databases under the Dutch Copyright Act:

The exceptions and limitations to copyright as implemented in the DCA all apply without prejudice to copyright protected databases. Not all are relevant of course, the exceptions/limitations that are can concern (I) temporary acts of reproduction (5(1) InfoSoc Directive), (ii) private copying (5(2)(b) InfoSoc Directive, (iii) reproductions by libraries, archives and museums (5(2)(c) InfoSoc Directive, (iv) illustration for teaching or scientific research (5(3)(a) InfoSoc Directive, (v) use for public security purposes (5(3)(e) InfoSoc Directive) and (vi) use for research or private study (5(3)(n) InfoSoc Directive).

Currently, no specific exceptions exist in the Netherlands. Of course, the new exceptions for scientific and commercial text- and dataming from the DSM Directive (articles 3 and 4) are being implemented.

Protection of databases under the Dutch Database Act:

The lawful user of a database that is made available to the public in any manner whatsoever may extract or re-utilize a substantial part of the content of the database without the authorization of the producer of the database if: a. the extraction of the content of a non-electronic database is for private purposes; b. the extraction is for illustrative purposes in connection with teaching or scientific research, provided that the source is indicated and insofar as the extraction is justified by the non-commercial purpose to be achieved; or c. the extraction or re-utilization is for purposes related to public security or an administrative or judicial procedure.

There is no specific compulsory licensing provision under the Dutch sui generis protection regime. Nevertheless, a decree of the Dutch Competition Authority can effectively result in compulsory licensing. Abusing a dominant position is prohibited under Dutch competition law (and European Competition Law). Recital 47 of the Directive also makes clear that sui generis protection may not promote abuse of a dominant position and that Community and national competition laws may be employed to avoid such abuse. Whether a refusal to grant a licence will be regarded as abuse under Dutch competition law will depend on the circumstances of the case. Taking advantage of a dominant position is not abuse per se. Enforcing an intellectual property right will be regarded as abuse only in exceptional circumstances.

The new exceptions for scientific and commercial text- and dataming from the DSM Directive (articles 3 and 4) shall also apply to sui generis databases.

4) Are databases protected by any provision other than a property right / IP right? If yes, please answer the following sub-questions:

a) What type of protection is available?

A database can be protected as a trade secret.

b) What are the requirements for such protection?

A database can be protected as a trade secret when it meets the requirements set out above under I 2. B)

c) Who is the person or entity entitled to this protection?

Any natural or legal person lawfully controlling a database as a trade secret.

d) What acts are prohibited for third parties to avoid infringement?

Please see the answer under question 2.

e) Does your legislation/case law contain specific exceptions to this protection (e.g. access right for data mining, scientist research, etc.)?

The acquisition of a trade secret shall be considered lawful when the trade secret is obtained by any of the following means:

(a) independent discovery or creation;

(b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;

(c) exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national laws and practices;

(d) any other practice which, under the circumstances, is in conformity with honest commercial practices.

The acquisition, use or disclosure of a trade secret shall further be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law.

The measures, procedures and remedies provided for in this Directive are dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

(a)for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media;

(b)for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;

(c)disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise;

C. Public Sector Information (PSI)

5) Does your legislation contain regulation/case law regarding PSI? if YES, please explain.

Yes, The Netherlands have implemented a Law on the re-use of public sector information ("Wet hergebruik overheidsinformatie") pursuant to Directive 2013/37/EU amending Directive 2003/98 on the re-use of public sector information.

6) Is there a right to access such PSI?

Yes, based on this Law on the re-use of public sector information anybody can file a request for the re-use of specified information. It is not required to have a specific interest in the information. Some information is excluded such as information with regard to which third parties own an IP right and information of educational and research institutions.

D. Health data

In the absence of a definition of "health data", for the purpose of this question this is considered to be data generated and/or collected in connection with medical treatment or medical research (such as clinical trials).

As per the study question note, this question does not address privacy and personal data aspects. This question also does not address aspects relating to approval for products or procedures, such as pharmaceutical approvals and the like.

7) Does your legislation contain regulation/case law regarding health data? If YES, please explain.

Under Dutch law, there is no tailored legislation or case law addressing the question if, and if yes to what extent, health data is protected by IP rights.

In the context of medicinal products, Directive 2004/27/EC and Regulation 726/2004 provides rules regarding the dossier (including e.g. clinical trial data) filed by a party with the marketing authorisation authority for the purpose of obtaining a marketing authorisation. Under these rules the dossier during an eight-year period is not accessible for third parties (the data exclusivity period). Thereafter the holder of the dossier is in principle obliged to release the dossier to companies wishing to develop generic versions of the medicinal product.

In the particular context of clinical trials, additional regulations apply, primarily pursuant to EU law, i.e. Regulation 726/2004/EC, Directive 2003/63/EC and the "*Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)*."[5] The EMA Guideline contains wording that suggests that there is such thing as an owner of the clinical trial data.[6] The concept of such ownership is, however, not further addressed, except that the EMA Guideline seems to assume that the owner of the clinical trial data would be the sponsor of the clinical trial.

8) Is there a right to access such information?

Under Dutch law there is no tailored legislation or case law addressing the question if, and if yes to what extent, health data can be accessed (other than in the context of personal data, see Q7 above).

In the particular context of clinical trials, the EMA, in accordance with EU law (as referred to above), has set out a policy on the publication of clinical data.[7] The policy follows the line of an EU Regulation on clinical trials which has been adopted but yet has to entered into force.[8] The main principle laid down by the EMA is that clinical trials data are made available to the public through a publicly accessible database, subject to (i) personal data and (ii), commercially confidential information. In two recent rulings[9], the Court of Justice (EU) has confirmed that based on Regulation 1049/2001/EC (concerning the public access to documents) and EMA's own policy, clinical trial reports cannot as such be considered commercially confidential information.

[5] https://www.ema.europa.eu/en/documents/scientific-guideline/guideline-content-management-archiving-clinical-trial-master-file-paper/electronic_en.pdf.

[6] *See inter alia Directive 2003/63/EC, 5.2 under c; Guideline, p. 15 and chapter 6.4.*

[7] https://www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use_en.pdf.

[8] *Regulation (EU) No 536/2014 of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC.*

[9] *C-175/18 (PTC Therapeutics International Ltd v EMA) and C-178/18 (MSD Animal Health v EMA).*

II. Policy considerations and proposals for improvements of your Group's current law

Could any of the following aspects of your Group's current law or practice relating to rights in data be improved? If YES, please explain and answer each of the sub-questions.

9) Protection of mere data?

The Dutch Group has heavily debated this question. The group is of the opinion that the protection of *undisclosed* Data through trade secret protection can be considered adequate since the coming into force of the recent trade secret legislation (described under I.2).

Relying on trade secret protection, however, severely restricts the marketability of data and could lead to data not becoming available to the public at all. That would harm innovation.

With regard to Data that are (to be) published, in some cases sui generis database protection can be invoked (depending on the exact definition of Data (see general introduction above)).

The Dutch group has identified three practical difficulties with applying database protection rights to mere data / big data.

The first is the requirement of "substantial investment" in the database. Case law shows that this criterion for protection is relatively vague. During litigation the quantum of "substantial", and which type of costs count towards it, is almost always debated. Substantial issues also arise with regard to proof. It is often difficult to furnish sufficient proof of the investment, especially when the requirements of the database protection right require that a distinction is made between the costs of building the database and presenting its contents, versus the costs of creating the elements that it contains. Outside the context of litigation, the unclarity about this requirement causes legal uncertainty: a database owner will not be able to know for certain whether he actually has a database right. Besides that, case law has shown that investments relating to the obtaining, verification or the presentation of mere data can in many cases not be taken into account because investments in these mere data have been made prior to creating “independent elements”: elements that can be separated from each other without affecting their independent informative content.

The second difficulty is that a database right requires that the collection is "arranged in a systematic and methodical way". Whilst caselaw shows that this requirement does not have a high threshold and is quite easily met for information collections that are readable for humans, the Dutch Group queries whether the criterion is flexible enough to even extend to data sets that have not yet been organized or structured. Such disorganized data is often used in AI and machine learning, with precisely the purpose to discover relations, correlations and structure where at first sight there is none.

The third difficulty is that database protection rights only arise in respect of collections of data. It does not afford protection for individual data (single unit of information) that is not part of such a set. From a fundamental point of view, the Dutch Group is of the opinion that if a right in mere data is to be recognized, it should be available to data elements that as such meet the requirements of the protection, irrespective of whether or not those data elements are collected into a set.

It is therefore clear that there is a rest category of Data that are created or captured thanks to substantial investments, which are not protected by any right once the Data are published.

According to the Dutch group, the question whether such data should be protected strongly depends on whether there is clear evidence from economic research that protection of Data would lead to more information / knowledge / innovation which could be valuable for society. If there is no clear evidence showing this, awarding protection is likely to have an overriding negative effect in the sense that it could stifle innovation.

If there would be clear evidence showing that protection of Data would lead to more information / knowledge and innovation, the Dutch group is in favor of a right protecting data. In that case protection should be relatively limited in time (a maximum term of 5-10 years) and could be tailored like the neighbouring right relating to sound recordings.

a) Requirements for such protection(s)?

Protection could be awarded, by law, when a substantial effort can be identified specifically aimed at the recording and / or storage of Data.

b) Ownership of the right(s)?

The right holder should be the (legal) person making the effort.

c) Scope of the protection?

The protection only covers the Data as stored (like a sound recording), has a limited protection period (5 years). The right would thus not, for the avoidance of doubt, cover the information that is embodied in and expressed by the Data. Only the data record should be protected (and any copies that are made of that record). Any party should be free to independently make its own measurements and data records. Such independently made data records may express the exact same information, but would not infringe on the data protection rights (for they are an independent record).

If one would take a recording of a soccer match as an example. This recording would comprise many (potential) data-elements. On the other hand, everybody watching (the recording of) the match could record / collect all kinds of Data about the match (Which players? How many corners? How many correct passes per player, the distance covered per player the amount of possession et cetera) independently. Depending on the data, probably not all data records will be identical. Software measuring the distance covered per player through the recording will probably result in slightly different Data than Data collected through a GPS sensor on the player. Even if the different ways of recording the Data would lead to identical values, the different data records should be protected individually to avoid an information monopoly.

The right would grant the right holder the right to prohibit third parties from reproducing, publishing, using, putting on the market or reselling, renting, delivering or otherwise trading in the Data.

d) Exceptions to this protection?

The scope of protection would not apply to:

- Private use
- Scientific / educational use

10) Protection of databases?

Although the threshold of protection can be considered vague, the database protection as implemented in The Netherlands pursuant to Directive (EU) 1996/9 is generally considered to be balanced by the Dutch group.

a**) Requirements for such protection(s)?**

b) Ownership of the right(s)?

c) Scope of the protection?

d) Exceptions to this protection?

11) Rules on contract law, *e.g.*, prohibition of contractual override, etc.?

No change is considered to be required.

12) Are there any other policy considerations and/or proposals for improvement to your Group's current law falling within the scope of this Study Question?

No.

III. Proposals for harmonisation

Please consult with relevant in-house / industry members of your Group in responding to Part III.

13) In your opinion, should the protection of mere data and/or database be harmonized? For what reasons?

Especially given the fact that the internet does not have clear State boundaries, the Dutch group considers it important that if any protection would be awarded to Data, such protection should be harmonized internationally.

If YES, please respond to the following questions without regard to your Group's current law or practice.
Even if NO, please address the following questions to the extent your Group considers your Group's current law or practice could be improved.

Protection of mere data
14) Should mere data be subject to a specific protection, *e.g.* an IP right or other type of right?

Please see above

15) If yes, what should be the requirements for such protection?

16) Who should be the owner of this right / IP right?

17) What acts should be prohibited to third parties to avoid infringement?

18) Which exceptions, if any, should apply to this protection (*e.g.* access right for data mining, etc.)?

19) What role should contract law play (*e.g.,* prohibition of contractual override)?

Protection of databases
20) Should databases be subject to a specific protection, *e.g.* an IP right or other type of right?

Please see above, the protection available in The Netherlands is considered balanced.

21) If yes, what should be the requirements for such protection?

22) Who should be the owner of this right / IP right?

23) What acts should be prohibited to third parties to avoid infringement?

24) Which exception should apply to this protection (*e.g.* access right for data mining, etc.)?

25) What role should contract law play (*e.g.* prohibition of contractual override)?

Specific regimes

26) Should Public Sector Information (PSI) be subject to a specific regime, *e.g.* regarding the control and access to such data/databases?

If YES, please explain the desirable regime.

27) Should health data be subject to a specific regime, *e.g.* regarding the control and access to such data/databases?

If YES, please explain the desirable regime.

There can be a public interest in the access to particular types of health data (such as clinical trial data) for the purpose of research and/or allowing generic manufacturing (see Q7/Q8). In this regard the Dutch Group also supports governmental and private initiatives to promote the pooling and exchange of certain health data between member states for such research purposes.[1] If Data were indeed granted a certain protection, the Dutch Group could imagine that such an (exclusive) right would, for similar public interest reasons, not extend to certain health data.

On the other hand, health data can exist in many different ways and forms. For instance, some data generated as a result of the increasing application of the internet of things may also qualify as health data. Such health data, the Dutch Group feels, would rather fall within the private domain, while also in this regard there can be merit in a voluntary cooperation and exchange of certain information (of course, each time subject to personal data compliance)

That said it seems that applying one specific regime to any health data in general would potentially have too far-reaching implications and not be appropriate for each and every type of such health data.

[1] See e.g. the EU Communication 25 April 2018 on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society.

General

28) Please comment on any additional issues concerning any additional aspect of Rights in Data you consider relevant to this Study Question.

--

29) Please indicate which industry sector views provided by in-house counsel are included in your Group's answers to Part III.

--