Special issue

Is it possible to place limits on the self-determination of your own genetic data? Certainly, and there is an urgent need for it!

*Iñigo De Miguel Beriain, Daniel Jove**

ABSTRACT: Voluntary disclosure of data is becoming an increasingly common practice. The problem is that these actions can seriously harm the relatives of those make such disclosures. This could happen with genetic data, which belongs to all persons about whom it provides information, regardless of who the sample donor is. What can be done in this situation? We defend the idea that they are the rights conferred by the GDPR to data subjects. On this basis, any processing of genetic data should be seen as an exercise of balancing interests, except where the need to respect professional secrecy requires otherwise.

KEYWORDS: DTC tests; voluntary disclosure of data; informational self-determination; collective data; data of relatives

SUMMARY: 1. Introduction: Family dinners, direct-to-consumer tests (DTC) and data protection – 2. Data protection, personal data and self-determination rights – 3. Genetic data are the personal data of different subjects – 4. Data protection as a tool for embedding conflicting interests – 5. First objection: The GDPR states that genetic data are only personal data of the sample donor – 6. Second objection: Data could become everyone's data because we are all related genetically – 7. Third objection: Until it is checked, we do not know if it is other people's personal data – 8. Fourth objection: If we accept the hypothesis, the research system would suffer terrible consequences – 9. Conclusion.

1. Introduction: Family dinners, direct-to-consumer tests (DTC)

Christmas Eve dinners are, in most western countries, a good time for family gatherings. They are meetings that often yield wonderful discussions in which, out of affection, the cousin we hardly ever see devotes himself to openly ragging two of his siblings or even his spouse even before dessert is served. There are, however, some years in which a confluence of stars brings about peace and harmony. For those for whom this situation will never be an acceptable scenario, it is more than advisable to bring up a hitherto underused resource to get the wheels turning: express your willingness to publicly disclose your own genetic data by publishing the results of a DTC on a public platform (Facebook, for example). This will display information on the presence of dominant pathological genes in your DNA, and the propensity for certain pathologies, and so on. As we all

* *Iñigo De Miguel Beriain: Ikerbasque Research Professor, IKERBASQUE, Bizkaia, Spain/Investigador Distinguido, University of the Basque. Mail: inigo.demiguelb@ehu.eus. Daniel Jove: University of A Coruña. Facultad de Derecho. Mail: d.jove.villares@udc.es. The article was peer-reviewed by the editorial committee.*

ISSN 2284-4503

share 12.5% of our DNA with our cousins, more so with our parents, descendants or siblings,[1] and these data could be used for very damaging purposes – whether it is to solve a crime, get a job or obtain medical insurance – it is quite likely that our goal of livening up the evening for the grandmother who has been disappointed by an untimely oasis of peace will be adequately fulfilled.

The example we have just given can (and does) happen in a world where DTCs are becoming increasingly common, clearly being a growing business.[2] If we add to this the fact that sharing even the most intimate parts of their lives on social networks has become a way of life for many people, our ability to access sensitive information increases substantially. Just think, some crimes are already being solved thanks to the use of DNA from family members, which has generated some ethical controversy.[3] The day when companies use tracking tools to value the genetic profiles made public by reckless, if not malicious, family members (or others) does not seem far off. Regardless of one's own prudence and rectitude, the indiscretion of others can be just as damaging.

In light of this scenario, there is an urgent need to analyse what we can do to protect the data we share with others, considering the limitations offered by current regulations, at least at European Union (EU) level. This will not be an easy task, as much of the legal discourse has been built based on the empowerment of the individual as an isolated subject. Therefore, it is often easy to arrive at excessive interpretations of the right to self-determination over one's own data. This approach is not the most appropriate to the principles of justice that require consideration of the interests of others in the exercise of one's rights. Furthermore, it is not an inevitable consequence of the application of the existing legal framework. On the contrary, it is possible and appropriate to draw the boundaries of determination for one's own data in accordance with the provisions of the General Data Protection Regulation (GDPR). However, we need to take this scenario seriously and explore the best means of dealing with voluntary disclosure that causes harm to third parties from a legal point of view. This article will be devoted to developing this argument.

2. Data protection, personal data and self-determination rights

Determining how we can defend ourselves against possible attacks on our privacy by third parties with whom we have the (dis)grace of sharing genes is not a simple issue. Voluntary disclosure scenarios place us in the eye of the hurricane of a struggle that confronts two different paradigms. On the one hand, a thought pattern is related to the paradigm of medical consent, which sometimes links the object to be protected – the information – with the subject that provides it, i.e. the sample donor. Based on this belief, it is considered that the right to informational self-determination should practically have no limits, as the data belong to the person who provides it and to no one else. For

[1] *Privacy implications of genetic data sharing*, available at: https://www.ecseq.com/blog/2019/privacy-implications-of-genetic-information-sharing (last visited 07/09/2020).

[2] S. THIEBES, P.A. TOUSSAINT, J. JU, J. AHN, K. LYYTINEN, A. SUNYAEV, *Valuable Genomes: A Taxonomy and Archetypes of Business Models in Direct-to-Consumer Genetic Testing*, in *Journal of Medical Internet Research*, 22, 1, 2020,1-16, DOI: 10.2196/14890.

[3] C.J. GUERRINI, J.O. ROBINSON, D. PETERSEN, A.L. MCGUIRE, *Should police have access to genetic genealogy databases? Capturing the Golden State Killer and other criminals using a controversial new forensic technique*, in *PLoS Biology*, 16, 10, 2018, DOI:10.1371/journal.pbio.2006906.

this reason, in the biomedical field, data are often treated as if it were an exclusive right of the person providing the sample, even though data protection regulations make it difficult to support this interpretation. On this basis, it would be very difficult (perhaps impossible) for relatives to raise an objection to the public display of a person's genetic data, as it is obvious that if the donor decides to publish genetic data from one of their samples, they would be exercising the right of self-determination over their data the law confers on them. This means of understanding the relationship of individuals with their genetic information therefore leads to a dead end.[4]

There is, however, a reasonable alternative to this status quo. However, understanding it means leaving the traditional medical law framework to enter the turbulent waters of data protection law. From this perspective, data are the object of a right that belongs to all subjects affected by the information transmitted, regardless of which, or who, the source is. In the context of the EU, this means taking as an unavoidable reference the GDPR, which regulates everything relating to personal data protection.[5]

Indeed, the paradigm constructed by the GDPR is based on a right: the right to informational self-determination, enshrined in Article 8 of the Charter of Fundamental Rights of the European Union (CFR). By virtue of this, it is the data subjects who decide on the destination of their data. However, this right does not confer unlimited powers on its holder, "but must be considered in relation to its function in society".[6] Actions such as voluntary disclosure must therefore be weighed against the rights and freedoms of other data subjects involved. In order to do so, we must balance the different elements involved in this scenario. To this purpose, two premises must be taken into consideration: 1) Some data may be the personal data of more than one person,[7] and 2) Therefore, if different data subjects express different views on a particular processing of these data (such as their publication on a social network), a conflict of interest – which will have to be resolved in each individual case – occurs. Next, we will explore each of these issues in depth.

[4] As Clayton et al. stated: "one of the most significant challenges is that many people take genetic data about themselves, which they often received from DTC companies, and post them online in an identifiable form to find their relatives, to share with other people with similar conditions, or to promote research. These actions necessarily reveal information about their relatives, as has been made clear by the use of GEDMatch to identity criminal suspects. At present, a person has no ability to prevent his or her relatives from revealing their own information. Moreover, there are no limits on who can access these data or for what purpose". In E.W. CLAYTON, B.J. EVANS, J.W. HAZEL, M.A. ROTHSTEIN, *The law of genetic privacy: applications, implications, and limitations*, in *Journal of Law and the Biosciences,* 6, 1, 2019, 1-36, DOI: https://doi.org/10.1093/jlb/lsz007.

[5] The GDPR is the most complete data protection standard. It offers the better system of guarantees, which makes it a reference model for other countries. Furthermore, thanks to its territorial scope, it is able to condition the processing models of those countries that intend to process data on EU citizens: Case C-362/14, *Schrems v. DP Commissioner*, ECLI:EU:C:2015:650; Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited y Maximillian Schrems*, ECLI:EU:C:2020:559, relating to Safe Harbour and Privacy Shield.

[6] Joined Cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR v. Land Hessen y Eifert v. Land Hessen y Bundesantalt fur Landwirtschaft un Ernahrung*, ECLI:EU:C:2010:662, para. 48.

[7] Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 45.

3. Genetic data are the personal data of different subjects

In general, it is often believed that personal data obtained from a biological sample belongs to the donor, who has an almost unquestionable right to decide on the information extracted from the sample – "my sample, my data". Conversely, the donor's relatives are often denied any prerogative over that information.[8] In our view, however, this concept is not compatible with the legal framework drawn up by the GDPR, as it is incompatible with the definition of personal data. Other errors are derived from this original error, such as the failure to recognize the rights (access, rectification, restriction of processing) that the data protection framework confers to the subjects whose personal data are being processed. This fact, on the other hand, ultimately leads to the vulnerability of those who are directly affected by the public disclosure of data obtained from the analysis of a sample that was obtained from a donor different to themselves. Thus, change is truly needed for this perspective. However, to do so, it is necessary to cement the linkage between information about a subject and personal data. This requires a deep understanding of the concept of personal data. Article 4 of the GDPR states that "personal data" means "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The concept of personal data, therefore, is broad and covers all types of information.[9] The key to determining whether the information obtained from a sample is a subject's personal information is whether, "by reason of its content, purpose or effect" that information is linked to a particular person[10] and, in that case, from which person. If it is possible to connect this information with a natural person, this information will be their personal data, without excluding other subjects.

The essential question, in short, is to determine whether the information extracted from a biological sample is personal data not only of the donor, but also of other people related to them. In the case of genetic data, and "to the extent that genetic data has a family dimension, it can be argued that it is "shared" information, with family members having a right to information that may have implications for their own health and future life".[11] They should therefore be considered the personal data of all concerned data subjects. The Article 29 Working Party has stated this, at least indirectly, by considering that the data collected from the samples of deceased people are considered their relatives' personal data, as "the information on dead individuals may also refer to living persons. […] Thus, where the information which is data on the dead can be considered to relate at the same time also to the living and be personal data subject to the Directive".[12]

---

[8] P. NICOLÁS, *Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos*, in *Revista Derecho y Genoma Humano*, extraord. number, 2019, 129-167.

[9] Case C-553/07, *Rijkeboer*, ECLI:EU:C:2009:293, para. 59.

[10] Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 35.

[11] A29WP, *Working Document on Genetic Data*, adopted on 17 March 2004, 8, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf.

[12] A29WP, Opinion 4/2007 on the concept of personal data, adopted on 20th June. The ICO has also stated explicitly that, "[i]n the case of requests for the medical records of a deceased person, it is possible that this could

However, if this is true for the deceased, it must also be true for the living, as the information is the same.

Therefore, the real issue is determining whether a data is personal and which individual's information it provides. In this regard, the source of the information – the biological sample, in this case – or the subject from which it was originally extracted is irrelevant (although it will be important for assessing conflicting interests). Thus, it must be concluded that the information obtained from the genetic analysis of donor samples is personal data of these subjects, but is also their relatives' data. Recognizing that certain information is personal data implies that the relatives receive the protection that the right to data protection confers, with the exceptions that the GDPR introduces regarding professional secrecy, which will be explained in the following sections. The question of which interest prevails if their interests diverge is different and will have to be resolved. There are sufficient mechanisms to proceed, as the next section shows. However, we cannot deny that a person has a right only because we do not know how to address the concurrent interests.[13]

4. Data protection as a tool for embedding conflicting interests

We have stated that genetic data might be the personal data of different subjects. This obviously means that there will be different wills involved in making decisions about them, and this means conflict. Therefore, we have to analyse whether this is an unsolvable problem, or whether it can be solved by the currently applicable legal framework. We adhere to the latter, as we believe that it is perfectly possible to resolve conflicts based on the GDPR. In this section, we will explain how.

Resolving conflicts of interest involves different variables that give rise to different scenarios. First, the legality of the controversial processing, that is, its legal basis, must be analysed. When this is not consent, the will of the interested party is not the decisive factor that justifies such treatment. In these cases, the interests of the data controller, the purpose of the processing, the public interest or the legal good to be protected are the elements that justify and condition the processing. At the same time, they are the criteria to be assessed in case of a possible conflict of interests between a data subject (A) who wants her data to be processed and a data subject (B), who has a different intention with regard to the same data (which also refers to her).

The resolution of this type of conflict may seem complex, but in practice it is not, precisely because the legal basis of processing and its conditions provide the necessary elements to carry out the balancing of interests. A wide variety of situations can arise. Let us imagine, for example, that a person performs, and pays for, a DTC, but does not want to share the results with her family members.

include genetic information which may also identify surviving relatives and thereby meet the definition of personal data under the Data Protection Act", available at: https://ico.org.uk/media/for-organisations/documents/1202/information-about-the-deceased-foi-eir.pdf.

[13] In addition, if there is a general interest objective that justifies a limitation of the rights of family members against the subject who provides the sample, it may be articulated by law, as long as the essential content of the right to data protection is respected and the measure is proportional. In this way, the legislator could give protection to certain situations (those in which there is a general interest that is properly justified) while the others are intended for the assessment of the conflicting interests. This action should be carried out, in the first place, by the data controller supported by the data protection officer (if any) and, if the dispute persists, by the supervisory authorities and, ultimately, by courts.

However, one relative, perhaps a clever nephew, decides to make use of the right of access and requests from the company that carried out the DTC that part of the information that may concern him. In this case, we would have, on the one hand, the aunt's interest in keeping secret, perhaps reinforced by a commitment to confidentiality, the company's own business model that could be prejudiced, and on the other hand, the nephew's right of access. In such a case, the right of access would probably not prevail, as the aunt's private life would be a difficult obstacle to overcome unless other reasons were provided in addition to the nephew's mere interest in knowing, not to mention what the GDPR stipulates about the duty to respect professional secrecy, which we detail later.

Let us now imagine that we have a case where the processing is necessary for the concluding a contract between the controller and data subject A, or to protect A's vital interests or for the fulfilment of a legal obligation. For data subject B to be able to prevent processing based on such grounds, her legal assets would have to be affected to an extent sufficient to outweigh the legitimate purpose of the processing. A different issue is data subject B exercising her right of access: this claim would have a better chance of success because it is an instrumental right, while allowing the data subject to exercise other rights,[14] such as the right to rectification (in order to rectify you must first know what information is being processed).

If the legal basis for a particular processing operation were instead the legitimate interest, the decision would be simpler. In these cases, data controllers must always carry out a prior analysis of the conflicting interests, as well as weigh the possible risks and effects on the rights and freedoms at stake. It would only be necessary to ensure that, in this assessment, they have considered the possible existence of more than one data subject with respect to the information with which they are dealing.

The solution, in short, depends on each specific processing. In any case, and in the final analysis, it will always be the data protection authorities or the courts who decide which interest prevails according to the circumstances. In other words, it would be necessary to analyse the different interests involved in each processing operation, the level of affectation of the rights, the purpose of the processing and the context of the processing itself.

Let us now imagine a complex case: the processing is based on the consent of one of the data subjects, the sample donor. In this case, the doubts are overwhelming. First of all, what are the obligations of the controllers? Must they obtain the consent of not only the person providing the information, but also of all those to whom it refers? Even if the answer were negative, even if we think that the consent of the donor is the only necessary consent, the controller would have to address the information duties corresponding to Article 14 of the GDPR. The legal answer, in short, depends on each specific processing. In any case, it will always be the data protection authorities or the courts that will decide which interest prevails in view of the circumstances. In other words, it would be necessary to analyse the different interests involved in each processing operation, the level of affectation of the rights, the purpose of the processing and the context of the processing itself. Therefore, in the case of genetic data, it should at least inform the next of kin (third or fourth degree), as this does not seem to be a disproportionate effort. Complex? Yes, no doubt, but the conflict could be resolved.

[14] Case C-434/16, *Peter Nowak v. Data Protection Commissioner*, ECLI:EU:C:2017:994, para. 57.

Furthermore, should the controller facilitate the exercise of the various rights (access, rectification, objection, etc.) to any data subject or only to the sample donor? If so, how should conflict situations be resolved? Once again, there are no general solutions applicable. In cases such as voluntary disclosure of genetic information on social networks and the eventual request of withdrawal by a relative, the resolution seems clear. The chances of the balance tipping in favour of the relative requesting removal are very high. Genetic data are special category data. Their processing, as a general rule, is prohibited (GDPR Article 9(1)), unless any of the circumstances foreseen in Article 9(2) of the GDPR applies. This means that the data subject who does not want to see this information published loses the additional protection afforded by the prohibition on the processing of GDPR Article 9(1). Of course, there will be situations where there may be reasons to justify such interference with the rights of an individual, but these will be the least. In most cases, the interest of the person who wants to make their genetic information no longer public should prevail. The slightest impairment of fundamental rights – both of the right to data protection and of others such as privacy or health – and the risk of discrimination will operate as reference criteria for elucidating conflicts between data subjects.

In any case, what is proven is that this approach from the GDPR legal framework provides criteria that make it possible to impose limits on some of the data disclosure we are analysing (especially the most disproportionate ones), as well as to bring peace to present and future family celebrations. This is despite the doubts regarding the measures that should be required from the processor or the complexity inherent in resolving any conflict of interest. However, we are aware that our proposal is complex and may generate opposition. For this reason, in the following sections, we analyse and respond to some of the possible criticisms thereof.

5. First objection: The GDPR states that genetic data are only personal data of the sample donor

The first objection to everything we have clarified so far claims that a genetic data is only a personal data of the sample donor because that is what the GDPR rules. This argument is based on Article 4(13) of the GDPR, which states that genetic data are data obtained, "in particular, from an analysis of a biological sample from the natural person in question". Moreover, Recital 34 states that "genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained".

These definitions, in short, fuel the idea that the information contained in the sample is only genetic data with respect to the sample donor. However, there are reasons for rejecting this option.

The first is that both formulas are not similar. The formula in the Recital emphasizes the origin of the data, but the fact that it ends with the phrase "or from the analysis of another element enabling equivalent information to be obtained" is revealing. It shows that the GDPR focuses on the information itself and not on the source or method of obtaining it. The definition in Article 4(13) reinforces this interpretation, as it does not appear to be exhaustive, but rather exemplary. The use of the

expression "in particular" instead of other options such as "only" and "exclusively" is a clear sign that the EU legislator did not wish to restrict the concept of genetic data to that with that particular origin, but rather to emphasise the more typical method of obtaining it.

Moreover, even accepting the argument that the definition of genetic data in the GDPR is restrictive, this would not deny the information its status as personal data, only the status as genetic data. In other words, we would not say that the data extracted from a biological sample are not personal data, as this conclusion would be incompatible with the definition of personal data, but rather that it would not be genetic data. However, such an interpretation would lead to the consideration that the GDPR would be differentiating two types of DNA-related data: genetic personal data, which would only be associated with the person providing the sample, and non-genetic personal data, that is, data that would provide information about a person, but would not be genetic because it did not originate from that person's sample, although the information would undoubtedly be genetic.

In our view, this interpretation is absurd. Let us imagine that genetic information comes from the sample of a person who has died but has a living twin brother. As is commonly known, this means that they share the same DNA. Thus, the information from one is the same as that from the other. Saying that a piece of information is not the personal data of twin B because it has been obtained from a sample of twin A, despite the fact that the information is equivalent, seems – is – totally incongruous.

In addition, if we review Recital 35 of the GDPR, we find that, among the data that can be considered "personal data concerning health" is "information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples". In this case, the GDPR advocates a broader consideration of what is health data. Note that it does not specify from whom the information comes, but talks about "a body part" rather than "his/her body part", and "genetic data and biological samples", not "his/her genetic data and biological samples".

In conclusion, this refutation is not strong enough to be taken into account, although it does at least raise a relevant query: the need to eliminate from the definition the phrase "in particular, from an analysis of a biological sample from the natural person in question", as it only generates confusion. If the legislator were to be embarrassed by such an action, he should at least emphasize its exemplary and not restrictive nature. However, the reason for advocating elimination is that there are currently much more appropriate definitions, such as that in Article 1 of Recommendation No. R (97) 5 on the Protection of Medical Data (February 13, 1997) of the Council of Europe.[15]

[15] Article 1 of Recommendation No. R (97) 5 on the protection of Medical Data (13 February, 1997) of the Council of Europe: "[t]he expression 'genetic data' refers to all data, of whatever type, concerning the hereditary characteristics of an individual or concerning the pattern of inheritance of such characteristics within a related group of individuals. It also refers to all data on the carrying of any genetic information (genes) in an individual or genetic line relating to any aspect of health or disease, whether present as identifiable characteristics or not. The genetic line is the line constituted by genetic similarities resulting from procreation and shared by two or more individuals".

6. Second objection: Data could become everyone's data because we are all related genetically

The second refutation of our proposal is based on the fact that we all share much genetic information with other people, beyond even our relatives. This makes it impractical to consider genetic data as the data of various data subjects. It would lead us to a scenario in which the GDPR could not be applied because eventually any genetic information extracted from an individual could be used to inform judgments about all other humans, and in turn all genetic groups.[16] So, it would be impossible for a data controller to take all groups into account.[17] Therefore, adopting this perspective means distorting the very idea of the right to data protection, which has been built on the basis of the defence of the individual, as a projection of their dignity and free development of their personality, that is, as an individual right, and not as a collective right.

This criticism, once again, is wrong. The GDPR has been applied efficiently to solve problems in which the rights of several data subjects concur on the same data, without resorting to the notion of supra-individual rights. In the case of genetic data, a fundamental factor must also be taken into account: the more distant the biological link, the less information is shared. This means that, in reality, the amount of information on which there may be a conflict will be equal to the percentage of DNA that is shared and the relevance of the information it reveals in each processing. In this way, the data referring to a dominant gene will not be the same as that referring to a recessive one. It will also be necessary to consider whether it is a gene that transmits probabilities of developing a pathology or whether it determines that a data subject will develop with total certainty. Similarly, it is also crucial to know for what the data is used. Processing can have very different consequences for different stakeholders. This evidence must be considered in the resolution of each concrete situation. It will be the context of the processing that "determines or influences the way in which that person is treated or evaluated"[18] and thus their chances of achieving, for example, access to or removal of that information, as discussed in previous sections.

A different – but more complex – issue are cases in which the genetic information extracted from an individual affects a whole community, or what the Article 29 Working Party terms the "biological group".[19] These are cases in which the analysis of an individual's DNA can reveal, for example, information about the lack of immunological resources to address a particular pathology in a community of human beings. Such situations are a more direct challenge of the assumptions of the GDPR, which

[16] E. T. JUENGST, *Groups as Gatekeepers to Genomic Research: Conceptually Confusing, Morally Hazardous, and Practically Useless*, in *Kennedy Institute of Ethics Journal*, 8, 2, 1998, 183-200.

[17] D. HALLINAN, P. DE HERT, *Genetic Classes and Genetic Categories: Protecting Genetic Groups through Data Protection Law*, in L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT, (eds.), *Group Privacy: new challenges of data technologies*, Dordrecht, 2017, 231, available at: https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf.

[18] A29WP, *Working document on data protection issues related to RFID technology*, adopted on 19 January, 2005, 8.

[19] A29WP, *Working Document on Genetic Data*, adopted on 17 March 2004, 6, Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf.

was constructed on the basis of the individual's defence.[20] However, this does not mean that such problems are unmanageable. Rather, it is important to address them as soon as possible. In fact, there are already regulatory precedents in this regard. Article 10 of the UNESCO Universal Declaration on the Human Genome and Human Rights, for example, states that: "[n]o research or research applications concerning the human genome […] should prevail over respect for the human rights, fundamental freedoms and human dignity of individuals or, where applicable, of groups of people".[21] The Article 29 Working Party state that developments in the understanding of genetics may mean a "legally relevant social group can be said to have come into existence – namely, the biological group".[22]

In our opinion, it would be sufficient to generate alternative guidelines to establish inclusion and exclusion criteria: if a data processing from an individual was intended to discover group vulnerabilities, it would be necessary to be particularly attentive to the bases of legitimacy of that processing and to the rights conferred on all affected people. In other words, the characteristics of the processing would condition both its performance and the security measures to be adopted. The impact assessments (Article 35) required by the GDPR are an adequate prevention mechanism to establish a firewall for avoiding undesired situations. In any case, it seems obvious that a calm reflection on the social, ethical and legal problems posed by group profiling is needed. A recent book edited by Linnet Taylor**,** Luciano Floridi and Bert van der Sloot[23] offers an excellent panorama on this issue. We would do well by following up on this basis.

7. Third objection: Until it is checked, we do not know if it is other people's personal data

This rebuttal denies the factual starting point: genetic data only correspond to the sample donors because we can only be sure that they yield reliable information about them and no one else. A similar certainty can only be obtained if a similar genetic analysis of a family member were carried out.[24] Therefore, and as there is no evidence that the information refers to the specific family member in a truthful way, we are not dealing with that family member's personal data.

This refutation, however, is based on the erroneous belief that only data that have actually been proven to relate to a person can be their personal data. In essence, this means accepting the idea that, in order to be personal data, the information must be true. However, there are data processing

[20] Indeed, as Hallinan and de Hert stated, "the link between an individual data subject and their personal data was established on the basis whether the data could identify him or her. Such an approach would be irrelevant in relation to genetic groups". D. HALLINAN, P. DE HERT, *Genetic Classes and Genetic Categories: Protecting Genetic Groups through Data Protection Law*, cit., 231. Available at: https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf.

[21] UNESCO, *Universal Declaration on the Human Genome and Human Rights*, 1997, §10.

[22] Article 29, *Data Protection Working Party*, 2004.

[23] L. TAYLOR, L. FLORIDI, B. VAN DER SLOOT (eds.), *Group Privacy: new challenges of data technologies*, Dordrecht, 2017, available at: https://www.stiftung-nv.de/sites/default/files/group-privacy-2017-authors-draft-manuscript.pdf.

[24] P. NICOLÁS, *Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos*, cit., 138, available at: https://www.bigdatius.com/wp-content/uploads/2019/12/05_Los_derechos_sobre_los_datos.pdf.

operations that produce effects on a person even if they contain erroneous information. As the Article 29 Working Party stated, "for information to be 'personal data', it is not necessary that it be true or proven. In fact, data protection rules already envisage the possibility that information is incorrect and provide for a right of the data subject to access that information and to challenge it through appropriate remedies".[25]

So, for example, if an insurance company can use a father's genetic analysis to make decisions about his children, even though they know it may not be accurate – they may not be genetically his – that information is the children's personal data (in addition to that of the father's) because it effectively determines how they are treated. As the European Court of Justice (ECJ) has noted, content, purposes and effects are factors that can determine the personal data status of a given piece of information, insofar as they connect it with a specific person on whom they project its consequences[26].

Accuracy or truthfulness are therefore not a precondition for the consideration of information as personal data. Whether the data protection regulations provide for remedies to rectify erroneous information (accuracy principle and right to rectification) is a different matter. What is obvious in any case is that in order to modify them, we must first accept that they are personal data. Otherwise, they would remain in a legal limbo that would be extremely detrimental to the data subjects, as such data would generate effects but we would have no mechanisms for correcting them. The essential point, in short, is that this information "is used to determine or influence the way in which that person is treated or evaluated".[27] If this is the case, then we are referring to personal data. And Thus, as can be understood, and as the examples that have been used throughout this paper demonstrate, genetic data can produce effects beyond that on the donor of the sample from which the information originates. Therefore, this refutation is clearly feeble.

8. Fourth objection: If we accept the hypothesis, the research system would suffer terrible consequences

The last refutation we analyse argues that we should dismiss the idea that data from a sample are personal data of the donor's relatives because its practical effects would be untenable: the use of data for health care or for research would become impossible. As there are multiple data subjects, it would be necessary to ask not only for the consent of the sample donor, but also that of all the other subjects who could be affected by the information gathered, which would greatly complicate the research. Similarly, patients could refuse to undergo tests necessary for preserving their health if they believe that such information could be provided to their relatives.[28]

[25] A29WP, Opinion 4/2007 on the concept of personal data, adopted on 20 June, 2007, 6, available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

[26] See Nowak case. In doctrine, S. WACHTER, B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, in *Columbia Business Law Review*, 2, 2019.

[27] A29WP, Working document on data protection issues related to RFID technology, adopted on 19 January, 2005, 8.

[28] C. GIL, *Utilización de muestras biológicas de origen humano con fines de investigación*, in *Revista de Bioética y Derecho*, 25, 2012, 19-32, available at: http://www.ub.edu/fildt/revista/pdf/RByD25_ArtGil.pdf.

There are several reasons, however, to consider that this objection is also inconsistent. To begin, it is not true that considering that the data of a sample are the personal data of the sample donor's relatives implies that they share the same rights as the sample donor. Article 14(5)(d) of the GDPR excludes the obligation to transmit information on the processing to data subjects "where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy". Therefore, professional secrecy operates as an instrumental guarantee of the right to data protection and allows for the circumvention of the obligation to inform the relatives in cases of medical diagnosis or treatment. This protection also extends to the case of biomedical research, insofar as it would also be protected by the professional secrecy of those who provide the samples.[29]

This is reinforced by the provisions concerning the processing of special category data (including genetic data and health data), at least in the cases that fall under the circumstances of GDPR Article 9(2)(h). That is, treatments "necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

It is true that the lack of requirement to inform is limited to activities subject to the duty of secrecy, i.e. care or biomedical research. This means that when transfers are made to third parties or processing is carried out for other purposes, all data subjects must be taken into consideration, informed and their consent obtained[30] – if that is the basis for the original processing. But this is not, in our view, a problem, but rather the opposite: an essential mechanism for limiting the lack of access to information exclusively to cases where there is a clear justification for it. In all other cases, it is perfectly reasonable – and legally enforceable – to inform all those affected of the processing.

We must therefore banish the fear that inspires the objection that we are analysing. As stated earlier, the circumstances of the processing matter. They determine how the various interests involved in each processing operation are addressed. Therefore, not every processing of genetic data will auto-

[29] An example of this secret requirement is the article 5.4 of the Spanish Act 14/2007, 3 July, Biomedical Research. Translation: "Any person who, in the exercise of his or her duties in relation to medical care or biomedical research, to whatever extent, has access to personal data shall be bound by the duty of secrecy. This duty shall continue to apply even after the research or activity has ceased". Original text: "Quedará sometida al deber de secreto cualquier persona que, en el ejercicio de sus funciones en relación con una actuación médico-asistencial o con una investigación biomédica, cualquiera que sea el alcance que tengan una y otra, acceda a datos de carácter personal. Este deber persistirá aún una vez haya cesado la investigación o la actuación".

[30] In this sense, the article 5.2 of the Spanish Act 14/2007, 3 July, Biomedical Research, recognizes as interested parties the relatives of the source subject and establishes that their consent must be obtained for the transfer of information to third parties. Translate: "The transfer of personal data to third parties outside of the medical-healthcare activity or biomedical research will require the express written consent of the interested party. In the event that the data obtained from the source subject could reveal personal information about their relatives, the transfer to third parties will require the express written consent of all concerned". Original text: Art. 5.2: «La cesión de datos de carácter personal a terceros ajenos a la actuación médico-asistencial o a una investigación biomédica, requerirá el consentimiento expreso y escrito del interesado. En el supuesto de que los datos obtenidos del sujeto fuente pudieran revelar información de carácter personal de sus familiares, la cesión a terceros requerirá el consentimiento expreso y escrito de todos los interesados".

matically entail an obligation to transmit that information to all potential data subjects. If consent is the legal basis for data processing, considering that those data would also be the relatives' personal data does not mean that the researcher would need to obtain their consent to perform the research. In principle, medical and professional secrecy guarantees that the actual processing can be carried out, based on the exclusive consent of the sample donor, without infringing the rights of any data subjects. As the GDPR states, a major interest – medical secrecy – rules.

This is obviously the general framework provided by the GDPR. However, that there are cases in which the circumstances render it necessary to disregard such a confidentiality and to transfer certain information to an interested party other than the donor, as may be the case with AIDS patients, cannot be ruled out. In such a scenario, there was conflict between professional secrecy and the need to preserve the health of third parties, a conflict that was resolved in favour of the latter: if revealing secrecy meant that patients would refuse to undergo diagnostic tests, it would be a risk to be assumed, but it would be an imposition on the health of third parties. It is true that the case of genetic data is much more controversial,[31] but in our opinion, the conclusions should be similar. In fact, there are rules that provide that if the analysis of a sample reveals relevant information about the health of the sample donor's relatives, there is an obligation to communicate this information, even if the donor objects. It is even worth recalling some famous (and old) judgements, such as the case of 1999, in which the Italian Guarantor for the Protection of Personal Data allowed access to relevant genetic information to the descendant of a deceased person who had explicitly opposed it, considering that her right to health prevailed over the right to privacy of the deceased.[32]

Therefore, in each case, the different rights in conflict and the entity by which they may be affected will determine the answer. However, there is no doubt that, for the purposes of biomedical research, the GDPR offers a starting point that provides a sufficient level of confidence to not put the research system at risk.

9. Conclusion

If we are to draw any conclusions from this paper, the main one should be this: it is perfectly possible to defend ourselves against misuse of the right to self-determination over data that endangers our privacy. Nonetheless, this is the case only if we accept that a person's genetic data are undoubtedly their personal data, but also of all persons about whom they transmit information that might influence the manner in which that person is treated or evaluated.[33]

Based on this evidence, each processing operation – including that allowing a sample donor to disclose their data publicly – will require specific analysis, as the GDPR requires data controllers to take into account "the nature, scope, context and purposes of the processing operation and the risks of

[31] M. ROTHSTEIN, *Reconsidering the duty to warn genetically at-risk relatives*, in *Genetics in Medicine*, 20, 2018, 285-290, DOI: https://doi.org/10.1038/gim.2017.257; E.W. CLAYTON, B.J. EVANS, J.W. HAZEL, M.A. ROTHSTEIN, *The law of genetic privacy: applications, implications, and limitations*, cit., 1-36.

[32] Garante per la Protezione dei Dati Personali¸ *Dati inerenti allo stato di salute - dati genetici, Cittadini e società dell'informazione*, 1999 (8), 13-15, available at: https://bit.ly/3ezTYnc.

[33] A29WP, *Working document on data protection issues related to RFID technology*, adopted on 19 January, 2005, 8.

varying degrees of probability and gravity to the rights and freedoms of natural persons".[34] The right to data protection is sufficiently flexible to allow the resolution of the different conflicts that may arise, applying precisely the criteria that should inspire the design of all processing. In short, the legal debate should not be on the nature of the information, nor on the right to be applied, but on how to reconcile this evidence with the legal assessment of the legitimacy of the processing that may affect data subjects with opposing interests. However, this requires courageous action.

Some years ago, the Article 29 Working Party stated: "a new, legally relevant social group can be said to have come into existence – namely, the biological group, the group of kindred as opposed, technically speaking, to one's family. Indeed, such a group does not include family members such as one's spouse or foster children, whereas it also consists of entities outside the family circle – whether in law or factually – such as gamete donors or the woman who, at the time of childbirth, did not recognise her child and requested that her particulars should not be disclosed – this right being supported in certain legal systems. The anonymity granted to the latter entities raises a further issue, which is usually dealt with by providing that the personal data required for genetic testing be communicated exclusively to a physician without referring to the identity of the relevant individual. Given the complexity of the issues described above, the Working Party takes the view at this stage that consideration should be given to a case-by-case approach in deciding how to address possible conflicts between the interests of the data subjects and those of their biological family".

After all this time, we still do not have a legal solution for the conflicts that arise from the fact that genetic information provides relevant data about different people. In this scenario, the lack of regulation can lead to clearly abusive behaviour, where the right of self-determination over data is overly protected. In our opinion, this requires urgent intervention, which would not so much require a regulatory reform as a decisive application of the provisions of the GDPR. In particular, it requires the assumption that certain information can be the personal data of more than one person. This should be accompanied by the definitive incorporation of the content, purposes and effects criteria as the basis for identifying certain information as a person's personal data.

With these guidelines as a basis, all those affected by information relevant to their lives would have the status of data subjects and the rights that are inherent to that status. As has been shown throughout this work, the obstacles and objections that could be raised are perfectly surmountable. In short, it is not so much a question of innovating as one of having the courage to apply the rights and regulatory provisions we already have. Let us hope that we have the confidence and courage to use them.

[34] GDPR, Article 24(1).

ISSN 2284-4503