**An Ever-Evolving Global Challenge**

**Alessandro Tarducci**

Law, Bocconi University, Milano, Italy

E-mail: alessandro.tarducci@studbocconi.it

Published 27th of January, 2025

**Abstract**

In recent years, the use of biometric and genetic data has become increasingly widespread, particularly in the field of scientific research and the digitized landscape. This data, also used for public security purposes, has raised numerous legal issues related to the protection of privacy, especially in the context where the processing of such information crosses the field of the right to the protection of personal data. In particular, the collection and use of biometric and genetic data, such as fingerprints, facial recognition, and DNA analysis, pose technological and regulatory challenges, as they deal with unique and highly sensitive information about individuals.

The rapid development of this sector has made it necessary to regulate the processing of such data, so that it is used exclusively for legitimate purposes, and with the utmost respect for the fundamental rights and freedoms of individuals. This paper aims to explore the legal framework in force in the European Union for the protection of biometric and genetic data, with particular reference to Regulation No. 2016/679 (GDPR) and the LED Directive, comparing these rules with the US regulatory context and the implications of the increasing use of artificial intelligence technologies in the processing of this data.

Keywords: Integrity, Innovation, Responsability

**1. GDPR and processing of biometric and genetic data**

The processing of biometric and genetic data is a central issue in the legislation on the protection of personal data, in particular with the entry into force of the General Data Protection Regulation (GDPR) in 2016. This category of data has historically faced definitional uncertainties: until the introduction of the GDPR, the legal qualification of biometric and genetic data was subject to various interpretations, often leaving uncertainties for both data subjects and those operating in the technology and security sector.

Regulation no. 2016/679 has finally clarified the issue, providing a clear definition of “biometric data” in Art. 4: “personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data”. Therefore, it is personal information obtained through “specific technical processing”, which refers to the physical, physiological or behavioral characteristics of an individual, allowing unique identification.

Examples of biometric data include fingerprints, facial recognition, iris scanning, hand configuration, as well as graphometric signatures and voice characteristics. “Genetic data” are defined - again in Art. 4 of the aforementioned Regulation - as: “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”.

The use of biometric data has increased significantly thanks to the evolution of recognition technologies, finding application in various contexts, such as the security of electronic devices (e.g., authentication via fingerprint or facial recognition) and access to confidential workplaces. However, the collection and processing of such data pose important ethical and legal questions, related to privacy and the protection of individual rights. The potential for massive collection of personal information, coupled with the uniqueness of data such as DNA, implies the need for strict oversight and privacy protection mechanisms to ensure that individuals’ rights are respected.

The GDPR, in Article 9 (Processing of special categories of personal data), establishes a general prohibition on the processing of biometric data intended to uniquely identify a natural person. However, this prohibition is mitigated by a list of exceptions that allow the processing of such data in certain circumstances: the explicit consent of the data subject, processing in the context of employment relationships, the protection of the vital interests of the data subject, employment in legal proceedings or for reasons of particular public interest and scientific research. These exceptions highlight an openness on the part of the European legislator towards the use and circulation of personal data, albeit at the expense of the provision of rigorous protection systems.

In this context, the GDPR is proposed as a fundamental tool to ensure the responsible and secure use of biometric and genetic data. The regulation provides for appropriate security measures to protect the fundamental rights and interests of individuals, aiming to build a solid foundation of precautions in the processing of such data. Furthermore, the Regulation recognises that biometric and genetic data are not only among the first indicators of the risks associated with the use of new technologies, but also highlight various ambiguities and uncertainties, which can affect the protection of individual rights, especially when their processing is required by the authorities, for the purposes of crime prevention and repression.

These considerations lead to an in-depth reflection on the opportunity to adopt an adequate discipline and outline a clear coordination between European regulations and those of individual states. It is essential to ensure that, despite the inevitable technological advancement and the increasing use of biometric and genetic data, human dignity is always preserved and fundamental rights are protected. The complexity of the balance between technological innovation and personal data protection underlines the importance of an integrated and attentive approach to the subject, so that the benefits deriving from the use of such data do not translate into privacy violations or discrimination.

Given these challenges, it is crucial to analyze the legal and regulatory implications for the protection of biometric and genetic data in the European Union and the United States, in light of the GDPR, the LED Directive, and the increasing use of artificial intelligence technologies. This examination will help determine whether current frameworks provide sufficient safeguards or whether further legislative interventions are necessary to address emerging risks.

**2. The CJEU’s ruling in Case C-205/21[[1]](#footnote-0)**

In this sense, it is necessary to focus on a practical case, in particular on the ruling of the Court of Justice of the European Union (CJEU) in Case C-205/21, which comes in a context of growing concern about the impact of technological progress on fundamental rights and freedoms. The Court was called upon to examine the compatibility of Bulgarian legislation on the processing of biometric and genetic data in criminal proceedings for tax fraud, raising questions of legal and “practical” relevance.

*2.1 Background and Preliminary Issues:*

The Bulgarian court, in view of doubts as to whether national law complies with EU law, stated the proceedings and referred several questions to the CJEU for a preliminary ruling.

These included the effective transposition into Bulgarian law of Article 10 of the LED Directive relating to the processing of biometric and genetic data for public security purposes, the compatibility of national legislation with Article 6(a) of the LED Directive regarding the obligation of coercive data collection in the event of refusal by the accused, and the legality of the systematic registration of biometric data such as photographs and fingerprints for all those accused of intentional crimes.

*2.2. Analysis of the Applicable Regulations:*

The CJEU has carefully examined the issue, first of all establishing that such processing, when aimed at the prevention and repression of crimes, is not governed by the GDPR, but by the LED Directive. This is confirmed in the recitals of the respective legislation, which clarify the scope of the Directive for criminal justice and public security purposes.

A crucial element of the decision concerns the need to clarify and specify national legislation on the processing of such sensitive data. In particular, it is emphasized that Article 10 of the LED Directive authorizes the processing of biometric and genetic data only in the presence of a clear justification of necessity, applying the “principle of data minimization”, provided for by the GDPR.

*2.3 Justification:*

It has been stressed that the collection of biometric and genetic data should only take place in exceptional circumstances, with a rigorous assessment of need. This requirement is essential to ensure the protection of personal data, especially in view of the interference that such practices entail with the right to privacy. The requirement of strict justification is particularly pronounced in these cases, as the data is sensitive in nature.

In addition, the CJEU stated that national courts must interpret domestic law in such a way as to comply with European regulations, thus ensuring that national provisions do not conflict with the requirements set out in the LED Directive.

*2.4 Conclusion:*

The Court concluded that referring national law to the GDPR, rather than to the LED Directive, does not preclude the possibility of authorising the processing of biometric and genetic data, provided that there is a clear and precise application of European rules. The CJEU has stated that the collection and processing of such data is lawful, provided that national law provides a clear legal basis and that the processing is deemed "strictly necessary", for the pursuit of objectives related to public security and the fight against crime.

Finally, the Court highlighted the need to ensure that disproportionate interference with fundamental rights does not occur, clearly distinguishing between categories of data and data subjects, in order to protect both victims and alleged perpetrators from unjustified processing.

In summary, the CJEU's ruling in Case C-205/21 highlights the importance of a careful balance between the use of technologies for public security and the protection of fundamental rights, reiterating the need for clear legislation and adequate safeguards for those involved in the processing of biometric and genetic data.

**3. Biometric and genetic data between GDPR and LED Directive: a comparison of disciplines**

The issue of the processing of biometric and genetic data raises crucial questions in relation to the European Union’s regulatory framework, which includes both the General Data Protection Regulation (GDPR)[[2]](#footnote-1) and Directive 2016/680 (LED Directive).[[3]](#footnote-2) These regulations share the objective of ensuring the protection of sensitive personal data, but differ in terms of scope and purpose.

The GDPR applies to the processing of personal data of individuals by private and public entities in general, regulating the use of data in a way that ensures adequate protection of individual rights. The LED Directive, on the other hand, focuses on the processing of data by competent authorities for the purposes of the prevention, investigation and prosecution of crimes, and aims to balance the protection of personal data with the effectiveness of cooperation between police and judicial authorities within the EU.

The main distinction between the two regulations therefore concerns the purpose of the processing: while the GDPR places a general prohibition on the processing of biometric data (art. 9), unless specific exceptions occur, the LED Directive allows the processing of such data in the criminal or public security fields, subject to strict conditions (art. 10). The Directive allows authorities to process biometric and genetic data for unique identification purposes, provided that such processing is strictly necessary and supported by appropriate legal safeguards.

A further difference concerns the practical application: the GDPR applies uniformly to all contexts of personal data processing, the LED Directive - on the other hand - leaves more discretion to the Member States on the specific regulation of the processing of biometric and genetic data, in the field of security. However, this freedom has created legal uncertainties, as two pieces of legislation coexist and both of which could be applied. An example of this is the case in Bulgarian law, where national rules do not seem to clearly distinguish between situations covered by the GDPR and those covered by the LED Directive.

The reference to Art. 9 of the GDPR in a context that should instead be regulated by Art. 10 of the LED Directive raises interpretative doubts: the Court of Justice of the European Union has clarified that the mere regulatory reference to the GDPR does not preclude the lawfulness of the processing of biometric data if it is clear, from national provisions, that such processing is regulated by the LED Directive and therefore falls within its scope. The Court emphasised that it is for the Member States to ensure that national legislation is sufficiently clear, precise and consistent to enable data subjects and courts to understand precisely the conditions of processing and the objectives pursued.

Ultimately, the harmonization between the GDPR and the LED Directive is a crucial point to ensure the protection of personal data and the efficiency of crime prevention and repression activities. Finally, the Court, through its case-law, recalls the importance of avoiding regulatory ambiguities and ensuring that the processing of biometric and genetic data is always carried out in compliance with the guarantees provided for by EU law.

**4. The principle of proportionality and the risk of prejudice to the rights of individuals**

The preamble to this may help to put the question of respect for the essential content of the rights and freedoms of the person concerned in a better context. It is therefore appropriate to ask whether the processing of biometric and genetic data satisfies the requirement to offer adequate safeguards for those rights and freedoms.

The principle of proportionality is central to the assessment of the impact of the processing of biometric and genetic data on the rights and freedoms of individuals. This principle serves as a balancing tool between the need to ensure public security and the protection of fundamental rights, as enshrined in Articles 8 and 16 of the Charter[[4]](#footnote-3) of Fundamental Rights of the European Union and the Treaty on the Functioning of the European Union (TFEU). The protection of personal data, including biometric and genetic data, is guaranteed as a fundamental right, and their processing must take place in compliance with this principle.

The use of biometric and genetic data by police authorities requires a delicate balance between security and individual rights. According to the principle of proportionality, any restriction on fundamental rights must be necessary, appropriate and targeted at a legitimate objective, such as public security or the fight against organised crime. Without such proportionality, there is a risk of seriously undermining fundamental rights, especially in a context where personal data represent an extension of the individual’s personality, as evidenced by Article 8 of the Charter.

The proportionality analysis requires that the police authority should use biometric and genetic data only when strictly necessary, avoiding less invasive alternatives, and ensuring that the processing is justified by an important public interest. The GDPR, through the principles of necessity, proportionality and data minimization, emphasizes that processing must be reduced to the minimum necessary to achieve the set objectives, thus protecting the privacy of the individual. To this end, authorities must apply appropriate technical and organisational measures in order to minimise the risks of misuse or unauthorised access to data.

European jurisprudence, as highlighted by the rulings of the Court of Justice, reiterates that restrictions on fundamental rights must be supported by clear and precise legislation, with adequate guarantees that prevent abuses. The absence of a proportionate and transparent justification for data processing leads to a violation of fundamental rights, creating a significant risk to privacy and personal freedom. Only in cases where organised crime is involved or there are serious threats to public security is interference with the rights of the individual justified. However, such interference must always be subject to strict judicial review in order to prevent abuse and ensure respect for fundamental rights.

**5. The processing of biometric and genetic data in the USA: the IV Amendment**

In the long debate that has long animated the legal reflection on the protection of personal, biometric and genetic data, the analysis of the legal issues related to the processing of this particular category of data cannot be disregarded, analyzing transversally, from a comparative perspective, the regulation on biometric and genetic data of the European legal system with that of the US legal system.

In particular, with reference to the examination of the regulation of biometric systems within the American system, it should be noted, as a preliminary point, that in the United States a single and complete federal legislation has not yet been implemented (despite the ambitious goal of adopting a federal text on *privacy* would seem — almost — to have materialized with the presentation of the first regulatory draft of the*The American Data Privacy and Protection Act [[5]](#footnote-4)* — ADPPA — formally introduced in the *House of Representatives* on June 21, 2022, still awaiting approval and which would seem to be inspired by the GDPR model) aimed at also regulating the collection and processing of biometric and genetic data, finding, rather, a fragmented state legal discipline adopted by the states of Texas, of Illinois and Washington.

In fact, the State of Washington in 2017, after that of Illinois and Texas, passed a biometric privacy law and, more recently, the State of California improved its regulation on *privacy*  protection at the end of 2018 with the *California Consumer Privacy Act* (CCPA)[[6]](#footnote-5), whose discipline to date has been amended by the *California Privacy Rights Act* (CPRA) passed in 2020, the latter law often presented as a potential model for a US Privacy and Personal Data Processing Act.

These provisions, however, highlight how the use of these systems is more popular in the public sector than in the private sector, where there is an orientation based mainly on strong deregulation.

This gives rise to a substantial paradox, such that the use of these systems, generally prohibited in public contexts, is instead increasingly normalized within private ones, with a privacy discipline that is decidedly less articulated than the discipline of the European GDPR.

On closer inspection, the US model focuses mainly on the processing of biometric and genetic data carried out for commercial purposes by private companies, and is, for this reason, decidedly more attentive to market practices.

As already mentioned, the incisive innovations that the biometric and genetic technology sector has undergone over the years have led to the progressive dissemination of such data in the various sectors of public and private action. Biometric systems have wide and varied fields of development and application. Currently, as already noted, one of the most widespread uses of this particular category of data, used above all in everyday life, concerns access to specific places or services as well as consent to the use of electronic devices in the most disparate sectors: banking, health, commerce, education and telecommunications. However, what is of particular interest here concerns the use of biometric data for the pursuit of purposes related to the fight against crime (the primary objectives of which are the prevention, investigation, detection and prosecution of criminal offences, including the safeguarding and prevention of threats to public security and the free movement of such data).

And it is precisely in this sector that these technologies play an increasingly incisive role. However, the constant development of these systems (especially biometric determination), within the various sectors, can prove to be highly problematic and involve numerous risks due to their use, especially with reference to respect for the fundamental rights and freedoms of its “users”.

Moreover, these data, an expression of the relationship between body and identity, have raised (and still raise) a series of fundamental questions both from an ethical and legal point of view. It follows that a disproportionate request for the use of such data, which goes beyond situations of strict necessity, would lead to an increase in threats to the protection of the privacyof individuals.

In order to trace the evolution of the discipline on biometrics, within the European and US legal systems, it is necessary to dwell on the strong relationship of the sector in question with the protection of privacy. In fact, if, on the one hand, the use of biometrics technologies aims to pursue positive results, on the other hand, this can cause negative effects that would impact people’s lives.

In this sense, it explains the reason why the growing and, by now, increasingly constant use of biometrics in the daily life of individuals has led to the belief that the framework of an effective regulation governing the security of these systems is essential. In this regard, it is believed that the development of a specific US regulation on biometrics would introduce and recognize greater protections for the rights and freedoms of individuals.

Therefore, if we want to make a comparison between the European and US legal systems, it should be pointed out that in the preparation of a regulation on biometrics, these systems adopt two different approaches. In the first, the adoption of the GDPR sets a solid and advanced discipline on *privacy*, in the second, however, there are still strong contradictions, as there is no single regulation placed to protect *privacy* and, above all, in the field of biometrics.

However, the draft text of the federal law instills hope by inserting a definition of both “*biometric information*” and “*genetic information*”.

In fact, the ADPPA presented to the US Congress, aimed at increasing privacy protection, would highlight some aspects and some provisions aimed at replicating the European privacy regulations, including the subject of biometric and genetic data in some articles.

The draft law defines “biometric information” as “any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including i) fingerprints; ii) voice prints; iii) iris or retina scans; iv) facial or hand mapping, geometry, or templates; or v) gait or personally identifying physical movements”. It also defines “genetic information” as “any covered data, regardless of its format, that concerns an individual’s genetic characteristics, including (A) raw sequence data that results from the sequencing of the complete, or a portion of, the extracted deoxyribonucleic acid (DNA) of an individual; or (B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph”.

On the other hand, in the European legal system, biometric data — in the past the subject of doctrinal reflections, but never expressly defined — with the introduction of the GDPR has finally obtained conceptual autonomy through a series of specific provisions (think of Art. 4, par. 14, GDPR, introducing an *ad hoc* definition as well as in Arts. 6 and 9 GDPR, relating, respectively, to the conditions of lawfulness for the processing and the processing of particular categories of personal data).

Despite this, regulatory gaps still exist with regard to the collection, storage and preservation of such information in databases (e.g. European agencies such as Eurodac and Europol that provide for the daily collection of biometric data of European citizens, and others, within security policies on illegal immigration or for the creation of a common biometric database at European level between the various police forces leaving Member States autonomy to adopt additional, stricter and more specific national rules used to address market regulation of these technologies.

These are data whose collection and storage, although not used to carry out control functions once acquired, could constitute a disproportionate interference with the right to privacy of individuals, especially if they are subjected to automated forms of processing and are stored in police databases.

However, in the European context, no member country has yet developed and introduced a primary-level legal framework for biometric and genetic systems. Therefore, the lack of specific national legislation on biometrics and genetics that complements the European model reflects the difficulties that these systems pose to national legislators (as happened in Bulgaria). From this it can be deduced, as a direct consequence of this aspect, the need to find a balance between the systematic processing of biometric and genetic data and the protection of individuals, which is not always so easy to pursue.

On the other hand, in the US legal system we are witnessing an approach that differs greatly from the presence of a single, rigid and targeted discipline on privacyand on the processing of biometric and genetic data, recognizing a wide space of autonomy to individual states.

For this reason, it seemed desirable to introduce some *privacy institutions* provided for by the European legislation into the US regulations.

Moving on, however, to the regulation of the processing of biometric data by public security authorities, while in the United States we are witnessing a very strong deregulation of these systems (attributing an extremely broad arbitrary power to federal and national agencies and bodies), in the European context, the use of biometric systems by public authorities is also regulated.

Yet there is an increasing number of public entities actively involved in the processing of biometric data for the purposes of crime prevention, security and counter-terrorism, which they can dispose of without any justification of their purposes and without having to incur any kind of limitation.

Specifically, although the federal government has long been promoting initiatives to collect biometric data, the absence of a set of precise rules in the adoption of biometric recognition systems reveals its fallacy. In fact, these technologies can significantly interfere in the protection of the privacyof the people involved, implementing real control and profiling actions and coming up against the possible (and probable) risk of interference of the primary purposes of security and public interest.

Furthermore, in the US system, the matter in which the rights and freedoms of individuals are most affected is that inherent in the processing of genetic data. The most common example is the one related to the collection of DNA samples. What in this context, is of particular concern concerns precisely the information on the body thus collected and all the consequences that this information entails on the individual. In addition, the archiving and, therefore, the storage in special databases, of this information allows large-scale searches to be carried out on suspects for indefinite periods of time.

This generates a violation of the individual's right according to the provisions of the Fourth Amendment of the American Constitution, highlighting the seriousness of the violation of physical integrity and *privacy* resulting from the taking of DNA samples from suspects.

In fact, DNA, considered one of the most powerful crime-solving tools for law enforcement, has undergone an evolution driven by the storage of a large amount of genetic data in *governmental, public and private databases, and the emergence of new techniques used to exploit these resources.*

A particularly widespread phenomenon in the US system is that it allows law enforcement authorities to increasingly use genetic databases, either by requesting the DNA profile of a suspect identified from a database or, more commonly, by comparing DNA taken from the crime scene with that stored in a database in an attempt to identify the suspect or a family member of the suspect.

Therefore, in such a context, the analysis of the discipline of the Fourth Amendment appears to be of fundamental importance, from the literal wording of which it follows that the attempt to assess society’s expectations in terms of *privacy* suggests that access to genetic information by law enforcement agencies is equal to or considered more invasive than searches that are carried out in homes, by checking SMS or emailand, more incisively, when a person's DNA is taken by law enforcement using databases for public safety purposes.

On the basis of this assumption, it can be inferred that both police access to non-governmental genetic databases and the use of covert methods to collect DNA require appropriate judicial authorization.

However, neither the collection of genetic samples nor their analysis and use by law enforcement agencies has been subject to specific regulation.

Significant, in this regard, is the well-known case *of Maryland v. King*.[[7]](#footnote-6) With this ruling, the Supreme Court ruled on the conditions of legitimacy of measures restricting personal freedom, subject to the guarantee provided for in the Fourth Amendment, and on the requests for the protection of privacy that they call into question. This case concerns Alonzo King arrested (charged and indicted) for assault in 2009 and subjected to the taking of a saliva sample, on the basis of the *Maryland DNA Collection Act[[8]](#footnote-7)*, which provides for the aforementioned operation against all subjects arrested, but not yet convicted, for a series of violent crimes. The genetic profile of the arrested coincided with a sample collected in 2003 and stored in the CODIS database (*Combined DNA Index System*, *software* that allows the organization of DNA data) for a sexual assault. This correspondence was used as the only evidence for the life sentence.

The defendant objected to the unconstitutionality of the Maryland law, which, by providing for an unreasonable limitation of personal liberty and not justified by a specific and circumstantial suspicion, would have violated the Fourth Amendment (which precisely protects the individual only from “unreasonable searches”).

King’s defense and the alleged unconstitutionality of the practice of DNA sampling by saliva swab were based entirely on the difference between this practice and the taking of fingerprints: while the purpose of the second intervention would be to identify the suspect, the DNA collection would have the sole purpose of finding a culprit for unsolved cases.

In this case, the need for the Court to balance the plurality of public interests worthy of protection that face the personal freedom and the right to privacy of the subject subjected to DNA collection is highlighted in detail.

The new investigative technologies have imposed on the Supreme American body “an *actio finium regundorum*, aimed at reconsidering the balance between security and freedom: on the one hand, they represent an instrument of unparalleled effectiveness through which the State carries out the tasks of social defense; on the other hand, their potential harmfulness cannot be ignored in the face of the individual’s claim to have an intimate sphere that cannot be reached by authority”.

The Court concludes, therefore, that the collection of DNA is a “*reasonable search”*, comparable to the taking of fingerprints and mugshots and, therefore, compatible with the Fourth Amendment. It goes on to highlight how police forces can legitimately collect DNA samples from individuals accused of serious crimes (including “*violence, attempted crimes of violence, burglaries, or attempted burglaries*”).

From the examination, therefore, the US system, as regards the collection of personal data — biometric, but above all genetic — would seem much less restrictive, preferring the aim of fighting prevention and crime, and protecting individuals only in stringent and limited cases.

**6. Conclusion**

Whether it is the regulation of biometric or genetic data, the fact that Europe and the US exist in an altogether different world of interests when it comes to privacy, public security, and individual rights is undisputed. The European Union has introduced the GDPR and LED Directive, which offer a very robust, centralized framework that tends to hold towards stringent protections, transparency, and minimization of data processing, especially in the criminal justice area. Indeed, this type of regulation would pay attention to proportionality and would deploy safeguards against misuse for a type of

absolutely sensitive data. In contrast, the United States lacks a unified federal standard; thus, the landscape appears fragmented with state laws, most guided by free market interests concerning data protection and the lack of regulatory oversight of the commercial and public sectors. Case after case, Maryland v. King demonstrates that the United States generally avails itself to placing public safety above personal privacy in law enforcement applications at the expense of rigid individual protections.

Emerging out of the American Data Privacy and Protection Act (ADPPA), this trend may soon usher in federal standards that might come close to matching GDPR principles. Such a development is hence witnessing the shifting horizon of the world beyond which standardization towards unique dimensions of data privacy norms has inscribed an urgent need for remedial strategies and progressive frameworks that afford harnessing individual rights vis-a-vis technological advancements. However, the use and acceptance of biometric and genetic data will increasingly be manifestations of a common daily life, so that both the EU and the US will ultimately have to come to grips with continuing refinement of their respective legal architectures to further ensure that the laws in place do indeed protect privacy without sacrificing responsible innovation that is essential in a rapidly evolving digital world.

**Bibliography:**

1. Charter of Fundamental Rights of the European Union. (2012). Official Journal of the European Union, 2012/C 326/02.  
   <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT>
2. Court of Justice of the European Union. *Judgment in Case C-205/21 - Bulgarian Law on Biometric and Genetic Data in Criminal Proceedings*.  
   <https://eur-lex.europa.eu/legal-content/EN/SUM/?uri=CELEX:62021CJ0205_RES>
3. European Data Protection Board. *Guidelines on Biometric Data in the Context of the GDPR*. (2021)  
   <https://www.edpb.europa.eu/edpb_en>
4. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation - GDPR)*.  
   <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>
5. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences (LED Directive)*.  
   <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680>
6. American Data Privacy and Protection Act (ADPPA). *Draft legislation presented to the U.S. House of Representatives on June 21, 2022.* <https://www.congress.gov/>
7. California Consumer Privacy Act (CCPA). (2018). *California Civil Code Sections 1798.100–1798.199.* <https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV>
8. Maryland DNA Collection Act. *A legislative framework for collecting DNA samples from certain criminal suspects.* (2008)*.* <https://mgaleg.maryland.gov/mgawebsite/>
9. Maryland v. King, 569 U.S. 435. *Supreme Court ruling on DNA collection and the Fourth Amendment.* (2013) <https://supreme.justia.com/cases/federal/us/569/435/>

1. Court of Justice of the European Union. *Judgment in Case C-205/21.* Available at [62021CJ0205 - EN - EUR-Lex](https://eur-lex.europa.eu/legal-content/EN/SUM/?uri=CELEX:62021CJ0205_RES) [↑](#footnote-ref-0)
2. Regulation (EU) 2016/679 of the European Parliament and of the Council. Available at: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [↑](#footnote-ref-1)
3. Directive 2016/680 of the European Parliament and of the Council. Available at <https://lc.cx/98WeY-> [↑](#footnote-ref-2)
4. Charter of Fundamental Rights of the European Union. Available at [EUR-Lex](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT) [↑](#footnote-ref-3)
5. American Data Privacy and Protection Act . *Draft legislation presented to the U.S. House of Representatives on June 21, 2022.* Available at [Congress.gov](https://www.congress.gov/) [↑](#footnote-ref-4)
6. California Civil Code Sections 1798.100–1798.199. Available at: [Civil Code - CIV](https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV) [↑](#footnote-ref-5)
7. Maryland v. King, 569 U.S. 435. *Supreme Court ruling on DNA collection and the Fourth Amendment.* Available at: [Maryland v. King | 569 U.S. 435 (2013) | Justia U.S. Supreme Court Center](https://supreme.justia.com/cases/federal/us/569/435/) [↑](#footnote-ref-6)
8. Maryland DNA Collection Act. *A legislative framework for collecting DNA samples from certain criminal suspects.* Available at: <https://mgaleg.maryland.gov/mgawebsite/> [↑](#footnote-ref-7)