Special issue

From "familial searching" to "forensic genetic genealogy": New frontiers – and challenges – of DNA analysis in criminal investigations

Giulia Formici *

ABSTRACT: Since its discovery, DNA analysis has been an important tool in criminal investigations: the creation of national DNA databases, retaining the genetic profile of criminals, revealed to be crucial in solving serious crimes. In recent years, the expansive use of DNA analysis, together with scientific and technological progress, led to the development of new sophisticated investigative techniques, from the so-called "familial searching" to the more recent use of "forensic genetic genealogy", based on the exploitation of commercial genealogy databases by law enforcement authorities. Notwithstanding their effectiveness, these new instruments raise serious ethical and legal concerns: this paper aims at presenting these complex challenges, by underlying the need to strike a proper balance between the public interest to a rapid and efficient identification of unknown offenders and the dangerous shift towards "genetic surveillance".

KEYWORDS: DNA; genetic forensics; genetic genealogy databases; familial searching

SUMMARY: 1. DNA analysis and genetic databases: some preliminary information on the origins and functioning of a powerful crime-fighting tool – 2. The expansive use of DNA analysis in criminal investigations: ethical and legal implications of the *familial searching* technique – 2.1. Looking for "closeness" by endangering privacy, data protection, presumption of innocence and non-discrimination – 2.2. First efforts to enlighten the "shadow database" – 3. The controversial use of recreational genealogy databases in the US: emerging concerns – 3.1. The potentialities of *forensic genetic genealogy*: the *Golden State Killer* case – 3.2. *Forensic genetic genealogy* as an "outgrowth" of the *familial searching* technique: a way to step over safeguards regulating traditional DNA analysis? – 3.3. The Privacy Policies established by commercial genealogy companies and the limits of the "informed consent" – 4. How to avoid "genetic surveillance": paving the path towards a profound guarantee of "genetic privacy" – 4.1. The risks of a "universal database": some timid attempts of regulatory answers – 4.2. How to resist the temptation of "seeing into the life of citizens": prompting a thoughtful and pondered debate.

* *Postdoctoral Researcher in Public Comparative Law at the University of Parma. Mail: giulia.formici@unipr.it.*
The article was peer-reviewed by the editorial committee.

ISSN 2284-4503

1. DNA analysis and genetic databases: some preliminary information on the origins and functioning of a powerful crime-fighting tool

Since its first use in 1985,[1] DNA analysis has become a fundamental tool in criminal investigations. The so-called forensic genetics, based on the "ability to extract DNA profiles – a biological structure considered unique for every individual – from samples collected at crime scenes",[2] is of paramount importance to establish the unique "genetic identity" of an unknown perpetrator.

In order to expand the potentialities of forensic genetics, in the mid-1990s many Countries started to create national DNA databases retaining the genetic profiles of convicted persons and, in some States – depending on the different legislative solutions adopted –, also of arrestees, victims, missing people or persons of interests. These repositories can be accessed, at certain specific conditions, during criminal investigations for the purpose of comparing, through a mainly computerized process, the DNA sample and profile obtained from the crime scene or the victim's body to the genetic information stored in the national database, thus making it possible to identify the unknown offender in case of an exact positive match.[3]

Due to the very sensitive nature of genetic data, specific rules were approved by national legislators, disciplining the collection, retention ("eligibility criteria") and circulation of DNA profiles in national repositories and clearly establishing the conditions, procedural requirements and purposes which legitimize DNA databases to be accessed and used by specifically identified law enforcement

[1] In 1985, the Leicestershire police employed for the first time the DNA analysis to solve a violent crime (the rape and murder of two young girls). The "fathers" of the "genetic profiling" are Sir Alec Jeffreys, who discovered the first "genetic fingerprint" in 1984, and Peter Gill, who revealed the possibility to compare the DNA profile, developed from biological materials found on the crime scene, to a reference sample and profile belonging to a known person. For more information on the origins of DNA profiling and its use for criminal investigations, see, *ex multis*, G. CLARK, *Justice and science: trials and triumphs of DNA evidence*, New Brunswick, 2007; in Italian: L. SCAFFARDI, *Giustizia genetica e tutela della persona. Uno studio comparato sull"uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Milano, 2017.

[2] H. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, Singapore-Braga, 2020, 2. The authors clearly explain that "studies on the use of DNA for individual identification depends upon broad zones that exists between the genes that are generally called "non-coding DNA". These intergenic zones reveal specific chemical sequences that are supposed to be unique to each individual and therefore produce a "genetic fingerprint". Comparison of different genetic fingerprints enables us to observe whether different samples of DNA come from the same individual or different individuals. In short, each person"s DNA is unique, except in the case of identical twins", 46.

[3] The first forensic database was created in England, in 1995; according to a 2019 Interpol analysis, 70 Countries around the world have nowadays a national DNA database in place (INTERPOL, *Global DNA profiling survey*, 2019, https://bit.ly/39NpDPb). DNA databases usually contain only DNA profiles, whereas the biological samples and personal information related to the genetic profile are stored in a separate software or repository, for privacy and data protection reasons. For a broader analysis on the DNA databases" history and functioning, see P. MARTIN, H. SCHMITTER, P. SCHNEIDER, *A brief history of the formation of DNA databases in forensic science within Europe*, in *Forensic Science International*, 119, 2001, 225-231; M. HIBBERT, *DNA databanks: law enforcement"s greatest surveillance tool?*, in *Wake Forest Law Review*, 34, 1999, 767 ff.; N. VAN CAMP, K. DIERICKX, *National forensic databases: social-ethical challenges and current practices in the EU*, in *European Ethical-Legal Papers*, 9, 2007; R. HINDMARSH, B. PRAINSACK (eds), *Genetic suspects: global governance of forensic DNA profiling and databasing*, Cambridge, 2010.

ISSN 2284-4503

authorities.[4] These complex rules and limits have usually been highly debated and discussed, because of their ability to affect, on the one hand, citizens' rights to privacy, data protection, presumption of innocence and non-discrimination, and, on the other hand, the efficacy of DNA forensic techniques: the wider the eligibility criteria are, the bigger the repository will be. If it is correct to affirm that the databases' size has an obvious positive impact on the possibility to find an exact match, it is also worth underlining that the retention of a vast amount of genetic information exposes sensitive data to significant risks of abuses, from data breaches to function creep. Finding a proper balance between the efficiency of this investigative instrument and a proportionate and necessary intrusion into citizens' private lives has represented a serious challenge for legislators, asked to take delicate regulatory decisions, sometimes challenged before national and supranational Courts. For example, in the European context, a relevant role has been played by the ECtHR: in the landmark case *S. and Marper v. UK,*[5] the Strasbourg Judges declared the UK legislation regulating the functioning of the *National DNA Database* (NDNAD) in violation of Art. 8 ECHR in so far as it authorized a blanket, indiscriminate and indefinite retention of DNA profiles belonging to merely suspected individuals, not subsequently convicted of offences.

This proportionality assessment and the correct balance between competing private and public interests led to different legislative solutions across the European Continent. In general terms, comparative surveys and analysis underlined the presence of two main tendencies: the so-called "extensive" and "restrictive" legislations,[6] able to impact on both the dimension of the national DNA database and the percentage of the population whose genetic profile can be included in the repository.[7]

[4] Together with technical standards (the quality and characteristics of data inserted in the database) and the conditions DNA laboratories should respect in order to be allowed to process genetic data.

[5] ECtHR Grand Chamber, 4 December 2008, Applications n. 30562/04 and 30566/04. According to the UK PACE (*Police and Criminal Evidence Act 1984*), genetic samples and DNA profiles of originally suspected but then unconvicted people could have been retained with no time limit and irrespective of the nature and gravity of the offence. On this decision: C. NYDICK, *The British invasion of privacy: DNA databases in the UK and in the USA in the wake of the Marper Case*, in *Emory International Law Review*, 23, 2010, 609-650; C. MCCARTNEY, *Of weighty reasons and indiscriminate blankets: the retention of DNA for forensic purposes*, in *The Howard Journal of Criminal Justice*, 51, 2012, 245-260.

[6] For a vast comparative analysis of national DNA databases" characteristics, with a focus on the European Continent, see: R. BROWNSWORD, *Genetic databases: one for all and all for one?*, in *King"s Law Journal*, 18, 2007, 273 ff; S. WALSH, J. BUCKLETON, O. RIBAUX, C. ROUX, T. RAYMOND, *Comparing the growth and effectiveness of forensic DNA databases*, in *Forensic Science International: Genetics*, 1, 2008, 667-678; F. SANTOS, H. MACHADO, S. SILVA, *Forensic DNA databases in European Countries: is size linked to performance?*, in *Life Sciences, Society and Policy*, 12, 2013, 1-13; ENFSI, *Survey on DNA-databases in Europe*, 2016; L. SCAFFARDI, *Giustizia genetica e tutela della persona*, cit.

[7] The elements that should be considered in order to determine the expansive or restrictive nature of national legislation governing DNA databases" eligibility criteria are related to: the criteria regulating the deletion of DNA profiles (f.i. after the death of the convicted or after a specific amount of years from the end of the conviction); the possibility to retain DNA profiles of merely suspected people or arrestees; the conditions for collection and retention of DNA profiles of people convicted (for all crimes or only for certain types of violent crimes, considered particularly serious); the deletion criteria of biological samples from which the DNA profile has been extracted; the scope of access; authorities allowed to access DNA databases.

In the US, the discipline of national DNA databases is far more complex: the *Combined DNA Index System* (CODIS) – the "FBI's program of support for criminal justice DNA databases as well as the software used to run these databases" – [8] is composed of a plurality of *DNA Index Systems*, hierarchically organized (national, state and local).[9] Along with federal legislation, establishing the eligibility criteria for the collection and retention of DNA profiles in the *National DNA Index System* (NDIS), there are also 50 DNA-collection State laws, creating a very fragmented regulatory landscape. As regards the federal discipline, the NDIS expanded its dimension after the approval of the *DNA Fingerprint Act* of 2005, which authorized any federal agency to collect DNA samples – and subsequently retain DNA profiles – not only from already convicted citizens (as recognized by the *DNA Identification Act* of 1994), but also from people arrested or facing charges for federal crimes. At the States' level, different practices can be registered: although all States have laws obliging convicted people to provide a DNA sample and include the DNA profile in the CODIS as well as in States' databases, some States' legislations limit this obligation only for certain convictions (usually violent crimes such as sex offences).[10] A broad inhomogeneity concerns the arrestees' discipline, with profound differences regarding the type of offences for which samples can be collected,[11] the possibility to store juveniles' profiles, and the rules – and procedural requirements – governing the deletion of DNA samples and the expungement of DNA profiles from genetic databases in case an arrest doesn't result in a final conviction.[12]

[8] See the *FBI fact sheets*, available at https://bit.ly/3uqwPc2.

[9] For an in-depth analysis of *Local DNA Index Systems* and the flow of genetic data from this lower level to *State DNA Index Systems* (SDISs) and the NDIS, see K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, in *Whittier Law Review*, 29, 2008, 909-960.

[10] "Forty-eight States require the collection of DNA for any felony conviction, and forty-two States require the collection of samples for at least some misdemeanor convictions", A. NIETO, *Familial searching: how implementing minimum safeguards ensures constitutionally-permissible use of this powerful investigative tool*, in *Cardozo Law Review*, 40, 2019, 1768.

[11] According to a study of the NCSL (National Conference of State Legislatures), updated to 2018 (available at https://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf), 31 States authorize, under specific conditions, the collection of DNA samples from arrestees. It"s important to mention that some States require *probable cause hearings* to establish the existence of a probable cause able to justify the DNA samples" collection. In this regard, the US Supreme Court was asked to evaluate the legitimacy of the State of Maryland law, imposing the collection of DNA samples from persons charged (but not already convicted) with burglary or violent crimes and requiring a judicial officer evaluation on the existence of a probable cause for the arrest. The Supreme Court, in *Maryland v. King* (2013), affirmed that such provisions don"t violate the Fourth Amendment and that a correct balance between public and private interests is established. As Joh clearly stated, this decision resulted in "opening up many opportunities for DNA collection by the police that extend beyond the limits of serious offences or even the category of arrestees", E. JOH, *Maryland v. King: policing and genetic privacy*, in *Ohio State Journal of Criminal Law*, 11, 2013, 294.

[12] The federal law imposes the expungement of DNA profiles from the NDIS once a conviction is overturned or, with reference to arrestees, the charge is dismissed or results in an acquittal. Similar provisions are established at the States" level: according to the abovementioned NCSL Survey, 16 States "provide for the expungement of a DNA record upon the request of the individual; 13 States provide for automatic expungement", https://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf. It is worth underlining that when automatic expungement is not in place, the arrestee has the burden of requiring expungement: nonetheless, people are usually unaware of this possibility or don"t have the necessary capabilities to start the request procedure.

Relying on the brief but necessary overview provided in this introductive Paragraph, the paper will focus on the challenges and issues posed by two most recent expansive evolutions of DNA analysis in criminal investigations: on the one hand, the use of genetic forensic beyond the determination of an exact match in a national DNA database,[13] implementing the so-called *familial searching* technique; on the other hand, the use of DNA analysis beyond national databases' searches, employing direct-to-consumer commercial genealogy databases with the purpose of detecting long-range familial relationships.

2. The expansive use of DNA analysis in criminal investigations: ethical and legal implications of the familial searching technique

2.1. Looking for "closeness" by endangering privacy, data protection, presumption of innocence and non-discrimination

Notwithstanding the efficacy of DNA analysis and the creation of national DNA databases, the traditional genetic forensic technique soon revealed its limits: when an exact match between the DNA profile collected from the crime scene or victims' body and the ones retained in the national repository is not found, no new and useful investigatory leads can be obtained and, in the absence of other evidence, the case risks to grow cold.

Starting from these premises and willing to exploit all the potentialities of genetic information, law enforcement authorities, together with geneticists, tried to develop innovative methods for testing and analysing genetic evidence. The so-called *familial searching* is one of the first sophisticated and controversial techniques deriving from an extensive use of DNA analysis and the adoption of different search parameters: unlike the traditional and routine searches in DNA repositories, looking for an exact match, this new investigative tool aims at detecting the likelihood of *genetic relatedness* through a low-stringency search. Based on the well-known genomics principle according to which we all share a significant portion of our genetic profile with other family members, this technique allows law enforcement agencies to find close relatives – siblings, parents and children – of the unknown offender by searching for a partial match[14] in the national DNA database, thus permitting to restrict the pool of potential suspects. In other words, *familial searching* represents an alternative and deliberate way of testing genetic information already stored in a criminal DNA repository,[15] different

[13] In the next Paragraphs, the general term "national criminal DNA database" will be used to refer to DNA databases run by public law enforcement authorities, mainly including convicted criminals, although, as previously seen, arrestees" or suspects" DNA profiles could also be included in these repositories, according to certain States laws.

[14] "A partial match suggests that the perpetrator of the crime and the offender in the database are related. [...] The greater the number of loci shared between two individuals, the greater the likelihood that the two individuals are related to one another", K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, cit., 922. For a very technical analysis of the technical functioning of *familial searching*, see also R. MATEEN, M. SABAR, S. HUSSAIN, R. PARVEEN, M. HUSSAIN, *Familial DNA analysis and criminal investigation: usage, downsides and privacy concerns*, in *Forensic Science International*, 318, 2021, 1-6.

[15] In other words, "In crime investigations, familial searching is defined as the intentional search of an offender DNA database for inexact matches between DNA evidence profiles and offender and arrestee DNA profiles. Upon the identification of one or more partial match profiles, law enforcement may investigate a purported

from a random partial matching.[16] The efficacy of this instrument depends upon different elements, among which the dimension, the eligibility criteria and the accuracy of national DNA databases: the bigger a national database is, the more the possibilities to find partial matches with already convicted criminals' profiles.

In recent years, a lot of newspapers reported an appreciable number of crimes solved using the *familial searching* technique,[17] mostly in the UK and US, and especially with reference to the so-called "cold cases"; in addition, law enforcement authorities underlined the fundamental impact of *familial searching* for investigations concerning missing people or for dismissing charges against wrongfully convicted people or suspects.

Despite these positive impacts, the technique has been profoundly debated by academics, legislators, Courts and civil society. As highlighted by many Civil Liberties Groups, *familial searching* implies the creation and exploitation of a sort of an unofficial "shadow DNA database",[18] made of (partial) genetic information pertaining to innocent people who simply are in close kinship connection to convicted criminals.[19] The use of this "shadow database" permits to multiply the potentialities of genetic testing by extending the number of possible matches related to a single genetic profile: in other words, the sentenced offender become a "genetic informant", unintentionally and indirectly targeting strict relatives and subjecting them to testing and investigations – and eventually implicating them –. In this sense, the *familial searching* materialises in "an expansion of the net of genetic surveillance to [mainly innocent] persons whose genetic information would have remained private from the State has it not been for the actions of their blood relatives".[20] By doing so, this technique, if routinely applied, can be employed to circumvent limits and safeguards already provided for the "traditional" use, collection, retention and access to genetic profiles and ultimately raises serious legal and ethical concerns related to a proportionate and necessary impact on the rights to privacy, data protection, but also on the presumption of innocence and non-discrimination.

---

family member of the partial matches as suspects", J. KIM, D. MANNMO, M. SIEGEL, S. KATSANIS, *Policy implications for familial searching*, in *Investigative Genetics*, 2, 2011, 2.

[16] There is a relevant difference from the so-called "partial matching" technique, *per se* considered, and the *familial searching*: "partial matching frequently occurs by accident whether as recognized by an analyst or by a quality assurance measure; whereas familial searching is a deliberate database search for family members to generate investigative leads", R. WICKENHEISER, *Forensic genealogy, bioethics and the Golden State Killer case*, in *Forensic Science International: Synergy*, 1, 2019, 117.

[17] For some examples of famous crimes solved thanks to *familial searching*, see A. NIETO, *Familial searching: how implementing minimum safeguards ensures constitutionally-permissible use of this powerful investigative tool*, cit., and in K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, cit.

[18] This suggestive expression has been used by E. MURPHY, *Relative doubt: familial searches of DNA databases*, in *Michigan Law Review*, 109, 2010, 291-348 (see also, E. MURPHY, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, in *California Law Review*, 95, 2007, 1-71).

[19] The genetic information could also be referred to individuals merely suspected or arrested, depending on the rules governing the database"s eligibility criteria, as underlined in Paragraph 1.

[20] H. MACHADO, S. SILVA, *What influences public views on forensic DNA testing in the criminal field? A scoping review of quantitative evidence*, in *Human Genomics*, 13, 2019, 2.

If the legitimacy of a forced collection of DNA profiles from people convicted for a crime is highly undebated, considering that these persons have "forsaken their right to privacy",[21] the same cannot be said for other kinds of searches or genetic testing and analysis – such as the *familial searching* – that can lead towards the dangerous shift of a vast "genetic surveillance".[22] Moreover, this technique results having a stronger and more invasive impact on certain ethnic groups – such as black people and Hispanic –, due to the higher representation of minorities' genetic profiles in national DNA databases. Consequently, *familial searching* has been considered a dangerous investigative instrument, able to exacerbate, especially in the US context, already existent "disparities in the criminal justice system, in which arrests and convictions differ widely based on race, ethnicity, geographic location and social class".[23]

On the basis of these possible side effects and despite the potentialities of this instrument, able to invaluably support law enforcement authorities when all other possible investigative leads fail to identify a suspect, the opportunity to apply *familial searching* should be seriously and carefully evaluated, by also taking into proper account both the risks of false identification[24] and the elevate costs in terms of money, time and human resources required to assess and select that information really and concretely useful and relevant, among the vast range of results possibly produced.

2.2. First efforts to enlighten the "shadow databases"

Familial searching was first used as a crime investigation tool in UK in 2002 and immediately raised the attention of bioethicists, lawyers and civil society: the Nuffield Council,[25] in its Report "The forensic use of bioinformation: ethical issues", clearly highlighted doubts and perils deriving from the employment of the *familial searching* technique, urging for dedicated policies, a strong ethical oversight and detailed and independent researches both on its concrete usefulness and on the

[21] D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, in *Forensic Science International: Genetics*, 36, 2018, 203. According to an affirmed doctrine and case-law, in the US "pivot persons, who have been convicted of one of the classes of crimes under which a DNA sample can be compelled, have a reduced expectation of privacy that is substantially outweighed by society"s interest in identifying the offender [...] Two US Supreme Court cases have recognized that the rights of these individuals are diminished to the extent that their rights are fundamentally inconsistent with the needs and exigencies of the regime to which they have been lawfully committed", K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, cit., 937.

[22] This expression has been used by J. ROSEN, *Genetic surveillance for all*, in *Slate*, 17 March 2009.

[23] F. BIEBER, C. BRENNER, D. LAZER, *Finding criminals through DNA of their relatives*, in *Science*, 312, 2006. On this topic, see also D. GRIMM, *The demographics of genetic surveillance: familial DNA testing and the Hispanic community*, in *Columbia Law Review*, 5, 2007, 1164-1194.

[24] As Syndercombe Court reported, "a false Y chromosome match in the case of Chen Long-Qui, for example, led to him being wrongly imprisoned in Taiwan for four years. [..] Using this approach to uncover relatives may not be that simple if the relationship is more distant", underlining the technical limits and the intrinsic possible error rate that characterise this instrument (D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, cit., 203).

[25] The Nuffield Council on Bioethics is an independent body that evaluates and prepares studies on sensitive ethical issues related to biology, medicine as well as to the use of biometric and genetic data for scientific research or investigative purposes.

practical consequences for fundamental rights.[26] For these reasons, the Association of Chief Police Officers, the Home Office, the Information Commissioner and representatives from the Human Genetics Commission established specific rules and conditions upon which familial searches are allowed: although the details of this policy are not completely publicly available, surveys and consultations revealed that this controversial investigative technique should be approved – not automatically but on a case-by-case basis – by the UK Chairman of the Database Strategy Board,[27] only for serious crimes and only once all other possible – less invasive – instruments failed to reveal useful investigative leads.[28] The prior authorization procedure, aiming at avoiding the transformation of *familial searching* into a routine assessment, rely on the notions of "seriousness of crime" and "sufficient resources": the Chairman is required to assess not only the level of gravity of the specific case but also the concrete capabilities of law enforcement authorities – in terms of human resources, time and money – to fully develop useful investigative leads from the – usually complex and multiple results of the familial searches.[29]

[26] The Council didn"t recommend a total ban of this instrument, but suggested that this technique "is not used unless it is necessary and proportionate in a particular case", NUFFIELD COUNCIL, *The forensic use of bioinformation: ethical issues*, 2018, 79.

[27] The Strategy Board "provides governance and oversight over the operation of the NDNAD [...]. The Board comprises representatives of the National Police Chief"s Council, the Home Office, the DNA Ethics Group, the Association of Police and Crime Commissioners, the Forensic Science Regulation, the Information Commissioner"s Office, the Biometrics Commissioner, representatives from the police and devolved administrations of Scotland and Northern Ireland", in https://www.gov.uk/government/groups/national-dna-database-strategy-board.

[28] "In considering whether to approve the application, the Chairman will consider the nature and gravity of the crime and whether there is a need to explore every investigative avenue to identify the offender, as well as the availability of funding and resources to pursue the search", T. PIQUADO, C. MATTHIES, L. STRANG, S. ANDERSON, *Forensic familial and moderate stringency DNA searches. Policies and practices in the US, England and Wales*, Santa Monica, 2019.

[29] Since the precise conditions regulating the current policy on *familial searching* are not fully accessible, the public debate over this investigative instrument is only based on the few reports and surveys available: see for example C. MAGUIRE, L. MCCALLUM, J. WHITAKER, *Familial searching: a specialist forensic DNA profiling service utilising the NDNAD to identify unknown offenders via their relatives. The UK experience*, in *Forensic Science International: Genetics*, 8, 2014, 1-9; R. GRANJA, H. MACHADO, *Ethical controversies of familial searching: the views of stakeholders in the UK and in Poland*, in *Science, Technology and Human Values*, 6, 2019, 1068-1092; T. PIQUADO, C. MATTHIES, L. STRANG, S. ANDERSON, *Forensic familial and moderate stringency DNA searches. Policies and practices in the US, England and Wales*, cit. It should be noted that, according to an official report, "Since the technique was implemented in 2002, more than 200 investigations have been conducted, assisting in the resolution of about 40 criminal cases (data from 2012) in the UK", O. GARCIA, M. CRESPILLO, I. YURREBASO, *Suspects identification through "familial searching" in DNA databases of criminal interest. Social, ethical and scientific implications*, in *Revista Espanola de Medicina Legal*, 1, 2017, 26-34. Notwithstanding this relevant employment and the lack of transparency on the specific rules agreed by the different components of the UK Board, it is worth mentioning that the UK is one of the few European Countries having a specific *familial searching* policy. For the analysis of the disciplines adopted in other European States, see: O. GARCIA, M. CRESPILLO, I. YURREBASO, *Suspects identification through "familial searching" in DNA databases of criminal interest. Social, ethical and scientific implications*, cit.; H. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, cit. and T. PIQUADO, C. MATTHIES, L. STRANG, S. ANDERSON, *Forensic familial and moderate stringency DNA searches. Policies and practices in the US, England and Wales*, cit.

In the US, this investigative method has often been subject to specific policies and, in certain cases, even to a general ban: at the federal level, for example, *familial searching* cannot be conducted, but the FBI left room for different disciplines adopted at the States' level, with the limit that only States' DNA databases can be subject to such searches (consequently excluding the genetic information contained in the NDIS). In this context, Maryland and Washington DC[30] are the only States which approved specific laws prohibiting the use of *familial searching*. On the contrary, and similarly to the UK discipline, in California the first specific policy regulating this tool was approved in 2008: although it is *per se* allowed, this technique is limited only to most serious crimes and should pass the prior administrative control of dedicated *State-Committee*, comprised of scientists, attorneys and law enforcement agents, whose task is to evaluate if the results produced by the *familial searching* can be actually useful and if these searches are able to effectively contribute to opening new investigative leads; moreover, it is established that incidental findings – such as non-paternity – are not disclosed to local law enforcement authorities, so as to exclude unnecessary intrusions into the private sphere of potential suspects.[31] Most recently, the New York State's law enforcement agencies adopted in 2017 a *Familial Searching Policy*, requiring the District Attorney to certify that all possible investigative efforts have been made in order to avoid *familial searching*, which should be considered as a "last resort" to be implemented when all other – possibly less intrusive – investigative methods resulted unsuccessful.[32] The fragmented approach that characterizes the US regulatory panorama, dominated by inhomogeneous policies' choices and different levels of safeguards and limits, brings to light the disadvantages associated with the absence of a federal law, able to provide shared guidelines and restrictions on such a delicate investigative tool.

Notwithstanding the different attempts to "enlighten", through the adoption of specific safeguards and conditions, the "shadow database", the debate on the limits and risks represented by *familial searching* is still widely open: while some commentators concluded that "familial searches should be forbidden because they embody the very presumptions that our constitutional and evidentiary rules have long endeavored to counteract: guilt by association, racial discrimination, propensity, and even biological determinism",[33] other scholars have considered it acceptable to employ closeness searches

[30] The Search Code of Maryland established, in 2010, that "A person may not perform a search of the statewide DNA data base for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired", Public Safety Code § 2-506, lett. d). The 2012 Washington DC Code, § 22-4151, affirms that "DNA collected by an agency of the District of Columbia shall not be searched for the purpose of identifying a family member related to the individual from whom the DNA sample was acquired" (lett. b).

[31] E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, in *Forensic Science International*, 292, 2018, e6.

[32] Other States performing *familial searching* are Arizona, Arkansas, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin and Wyoming. For an in-depth analysis of policies and choices taken at the US States" level, see B. FIELD, S. SEERA, C. NGUYEN, S. DEBUS-SHERRIL, *Study of familial searching policies and practices: case study brief series*, ICF Paper, August 2017.

[33] E. MURPHY, *Relative doubt: familial searches of DNA databases*, cit., 34. The author has affirmed that "a Court might deem irrational a formal policy that effectively divides the population into two groups – those related to convicted offenders and those who are not – and then threats the former population as presumptive suspects in criminal investigations while exempting the latter population from such suspicion" (331). Murphy also criticized some of the policies and safeguards adopted in certain States to limit the impact of *familial searching*:

provided that stringent limits are determined, such as the proportionality of the intrusion evaluated on a case-by-case basis,[34] the seriousness of the crime[35] and the existence of proper procedural and privacy safeguards. Other commentators, on the contrary, rejected what have been defined as "myths and exaggerations"[36] regarding *familial searching*: this technique cannot be considered as equivalent to a "guilt by association" investigative method since it only represents an instrument to generate new leads and not a list of precise suspects. Moreover, according to Wah, relatives contacted by law enforcement authorities after a partial match has been found, "may decline to answer questions or leave",[37] so that any unreasonable search and seizure occur. Consequently, no constitutional issues derive from *familial searching*, *per se*: although a "humane system of criminal justice should strive to keep side effects to a minimum, consistent with the objective of convicting the guilty", "forgoing the opportunity to apprehend and prosecute wrongdoers also has grave costs. An advanced database system that includes highly accurate kinship matching is a permissible legislative choice", also considering that in almost all jurisdictions, specific rules preventing misuses of genetic data and ensuring a high-quality standard of laboratories and analysis are in place.[38] Finally, the same authors consider the discriminatory impact of the *familial searching* as a false affirmation: far from being related to this techniques, the over-representation of specific minorities in DNA databases is related to more profound and already existent problems affecting the criminal justice system; using DNA analysis such as the *familial searching* can, on the contrary, represent a

for example, "allowing executive branch officials - whether a governor, attorney general, or state laboratory administrator - to unilaterally authorize such a wide-sweeping and politically contentious form of searching is to grant the executive unchecked authority to dramatically expand the size and character of the DNA database", 341. Differently from other authors who considered the prior authorization a viable and useful safeguard, the idea of a mere administrative control by public authorities, such as the attorney general, is not considered a sufficient measure to avoid risks of abuses.

[34] See, among the others, S. SUTER, *All in the family: privacy and DNA familial searching*, in *Harvard Journal of Law and Technology*, 2, 2010, 310-399 and A. NIETO, *Familial searching: how implementing minimum safeguards ensures constitutionally-permissible use of this powerful investigative tool*, cit. The latter author, considering the choice of some US States not to allow *familial searching*, affirms that "if properly drafted and scrupulously monitored, familial searches policies have the potential to solve cold cases and exonerate individuals who have been wrongly convicted", thus expecting "law enforcement in States that have banned familial searches to urge lawmakers in their States to adopt such policies in the future", 1770. Both authors consider that, in the US context, *familial searching* would withstand a Fourth Amendment challenge.

[35] It is nonetheless worth underlining that some US States, such as Virginia, allow familial searches to be conducted against convicted criminals as well as arrestees. Other US States, for example Colorado, don"t limit *familial searching* to serious crimes "but requires that crime investigators submit written requests to conduct familial searching when the crime under investigation poses a substantial public safety concern and conventional investigative approaches have been exhausted", J. KIM, D. MANNMO, M. SIEGEL, S. KATSANIS, *Policy implications for familial searching*, cit., 6. The authors suggest some possible solutions and specific policies useful to increase efficiency without undermining fundamental rights, proposing some limitations – such as the creation of a specific ethical committee or a limited list of crimes legitimizing the use of *familial searching* – able to address legal and social concerns.

[36] D. KAYE, *The genealogy detectives: a constitutional analysis of familial searching*, in *American Criminal Law Review*, 50, 2013, 160.

[37] K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, cit., 941.

[38] D. KAYE, *The genealogy detectives: a constitutional analysis of familial searching*, cit., 163. The author firmly opposes Murphy"s theories and her definition of "shadow database".

means to alleviate these issues: "investigators will be guided by the DNA evidence, which holds no preconceived notions, stereotypes or biases about racial, ethnic or social groups and classes".[39]
This ongoing debate appears as the result of a dichotomy between public safety and efficiency of law enforcement activities, on the one hand, and fundamental rights' guarantees on the other hand, that urgently requires the assessment of a clear balance-point.

3. The controversial use of recreational genealogy databases in the US: emerging concerns

3.1. The potentialities of forensic genetic genealogy: the Golden State Killer case

In recent years, the ethical and legal debate arisen from the extensive use of DNA analysis through the *familial searching* technique has witnessed a significant and cumbersome development: the emergence of what has been significantly named *forensic genetic genealogy.*[40] This new investigative instrument exploits the great potentialities of genetic genealogy and, in particular, the unprecedented source of information represented by the commercial and recreational genealogical databases, run by private companies. Differently from traditional forensic DNA analysis, "the power of genetic genealogy lies in the comparison process and the ability to search for genetic matches in databases", by combining genealogical research techniques with the information contained in DNA profiles for the purpose of detecting existent biological relationships.[41]

[39] K. WAH, *A new investigative lead: familial searching as an effective crime-fighting tool*, cit. 955. Seemingly, Nieto stated that "it is an unfortunate reality that the American criminal justice system is heavily racialized [...]. Familial searches are a part of this imperfect system, and until a massive overhaul of the criminal justice system truly changes this reality, it is left to states and law enforcement to ensure that their actions and policies provide equal treatment to the greater extent possible", A. NIETO, *Familial searching: how implementing minimum safeguards ensures constitutionally-permissible use of this powerful investigative tool*, cit., 1790. For these reasons, the author affirms that *familial searching* cannot be, *per se*, considered to have a discriminatory purpose and the adoption of appropriate safeguards can ensure sufficient guarantees of equality in the implementation of *familial searching* techniques.

[40] See, for example, C. PHILLIPS, *The Golden State Killer investigation and the nascent field of forensic genealogy*, in *Forensic Science International: Genetics*, 36, 2018, 186-188; D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, in *Forensic Science International: Genetics*, cit. Other authors use the term "forensic DNA phenotyping", referred to "a set of techniques that allow inferring genetic ancestry and externally visible characteristics of criminal suspects on the basis of a DNA sample", H. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, cit., 86.

[41] For a deep yet understandable explanation of how DNA testing and genetic genealogy work, see D. KENNET, *Choosing your DNA test: the best DNA testing kits*, May 2020, https://bit.ly/3dFBjor. It is worth mentioning that "traditional genealogy has been practiced for centuries, using documentary records and oral histories to trace families backwards in time. Until recently, they were the only ways to connect extended family members, but with the advent of direct-to-consumer genetic testing, it is now possible to find relatives through shared DNA", E.M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, in *Forensic science international*, 299, 2019, 104. From a very technical point of view, unlike the traditional forensic DNA analysis technique which uses *autosomal short tandem repeats* (so-called STRs method) in order to determine a genetic profile, genetic genealogy employs a great amount of *single nucleotide polymorphisms* (SNPs method) disseminated in the autosome, able to offer a vast variety of information, from the identification of distant relatives to the prediction of pathologies" predisposition (such as Alzheimer or mental diseases). This difference is strictly related to the very nature and purpose of the two different analysis" methods: if traditional DNA profiling used by law enforcement authorities aims mainly at identifying offenders and intends

Essentially, consumers of commercial genealogical services are asked to submit and upload a genetic sample – in some cases via cheek swab or spit kit, usually provided by the company itself, or in other cases a sample generated from other sources – to genealogy companies, such as AncestryDNA, 23andMe, MyHeritage and FTDNA, in order to obtain a DNA testing; this preliminary analysis, based on high-quality DNA sample – substantially different from the ones usually found on the crime scene, often small and of degraded quality –, is functional to a subsequent and delicate phase, that of the comparison of consumer's markers to other users' profiles stored in the company database. This second operation "provides the user with a list of DNA matches and a prediction of the possible relationship or range relationships based on the amount of DNA shared".[42] The more extended a direct-to-consumer company repository is, the more matches can be found.[43] Although errors and misattributed relationships are a concrete possibility, these DNA databases have become increasingly used to find unknown relatives and to build a precise family tree (descendancy research), also thanks to more affordable DNA testing costs.[44]

The spread and growth of these databases have inevitably augmented the number of genealogical records available online; this tendency has also led to the creation of open-data genomics DNA databases, such as GEDmatch: unlike direct-to-consumer companies, these services don't provide for genetic testing; they only guarantee a comparison between a DNA genealogy test, uploaded by the user, and the genetic data voluntarily made available by other consumers who opted in to share their profiles and identities. The algorithms employed by the online database allow a one-to-many query and research, returning the user a list of other customers whose DNA information presents more matches with, also specifying the estimated relationship and/or the amount of DNA shared.

For their potentialities, related to the quality of genetic data retained (the so-called "density" of genetic marker data) and the broad dimensions of the genealogical databases, these repositories and the connected genetic genealogy techniques have recently drawn the law enforcement authorities' attention, especially as regards cold cases' investigations: once a perfect match with the DNA profile of the offender cannot be detected in national criminal DNA databases, and/or the *familial searching* method has not been effective – meaning that no relatives of the offender have been subject to a conviction in the past or their DNA profiles have not been included in the criminal genetic database, the access to commercial genealogical repositories, by possibly giving information about the

to limit its impact on the intimate sphere of citizens, using only the less invasive STRs method, in contrast "SNPs are chosen precisely for their informational richness. People submit their DNA to sites like 23andMe or MyHeritage because they want to know more about their genetic make-up than just identity. 23andMe, for instance, offers information about disease carrier status, predictive wellness, and cosmetic conditions, relying on hundreds of thousands of SNPs rather than the 13-20 STRs in the typical forensic profile", E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e5.

[42] D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, in *Forensic Science International*, 301, 2019, 108.

[43] As underlined in the 23andMe website, "The 23andMe DNA database has more than five million genotyped customers worldwide. You will continue to find new relatives as our database grows over time", https://www.23andme.com/en-int/dna-ancestry/.

[44] "By February 2019 it was estimated that more than 26 million people had taken a direct-to-consumer genetic test. By 2021 there are likely to be over 100 million people in the direct-to-consumer databases", D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 108.

genealogy of the unknown offenders, can be a valuable tool, able to narrow the suspects' pool to a – or more – specific family tree.

It comes with no surprise that in recent years, genealogical databases have been used by US criminal investigators to detect new suspects' leads in numerous active cases or to "revitalize" cold cases – mostly related to missing people or serious crimes, some of which remained unsolved for decades – [45]. Among them, what has become famously known as the *Golden State Killer* case had the merit to shed light on this new investigative tool, by bringing the nascent technique to the public attention, stimulating a profound and paramount debate.[46]

In April 2018 the California police declared the arrest of Joseph James DeAngelo, accused to be the notorious serial killer and rapist of more than 50 women in California, from the 1970s to the 80s. Despite DNA samples – and consequently the profile – of the offender were found in multiple crime scenes, no match between the killer's DNA and the genetic profiles retained in the NDIS was found and no suspect was identified. For this reason, police investigators decided to upload the genetic profile of the offender on GEDMatch, by creating a false user account and identity:[47] the matching genealogical operations gave a considerable number of results, which were then employed by investigators, together with genealogists, to construct a potential offender's family tree and to gradually narrow, through traditional investigative techniques, a possible suspects list.[48] After months of complex researches, the police reached Joseph DeAngelo and, using a discarded DNA sample,[49] finally obtained a direct and exact match between the suspect's profile and the DNA found

[45] For some relevant case studies and examples of crimes solved thanks to the use of this particular technique, see D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit.; but also E.M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit., 110 ff.

[46] As underlined by Machado and Granja, "the case was considered by *Nature* one of the scientific events that shaped the year of 2018. Barbara Rae-Venter, a genealogist who helped to identify the golden State Killer, was distinguished by the same journal as one of the "ten people who mattered this year". According to *Time*, Barbara Rae-Venter "has provided law enforcement with its most revolutionary tool since the advent of forensic DNA testing in the 1980s"", H. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, cit., 91.

[47] While uploading the unknown offender"s DNA profile, investigators had to declare, according to the Terms and Conditions of the direct-to-consumer service, that the genetic data were either a) their own; b) that they were the legal guardian of the DNA donor or c) that they were authorized for other reasons. None of these affirmations were true in the *Golden State Killer* case.

[48] As reported by Kennet and by many newspapers which disclosed important details related to the *Golden State Killer* case, "several thousand hours of genealogical detective work" were required in order to "build" a clear family tree, starting from very distant matches (D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 107); on this point, see also R. CARROL, *Golden State Killer: hope for unsolved murder case as ex-cop arrested*, in *The Guardian*, 26 April 2018; G. KOLATA, *The Golden State Killer is tracked through a thicket of DNA and experts shudder*, in *New York Times*, 27 April 2018; J. JOUVENAL, *To find alleged Golden State Killer, investigators first found his great great great grandparents*, in *The Washington Post*, 1 May 2018.

[49] In the US, during investigations and without a consent of the interested individual, it is considered lawful to employ "discarded" DNA, namely an abandoned biological sample (for example the DNA found on a cigarette-tip or on a glass or a chewing gum). This is motivated by the enforcement of the so-called "third-party doctrine", related to the right to privacy and the Fourth Amendment protection: the idea is that once a biological sample is discarded, a person cannot invoke the existence of a "reasonable expectation of privacy"

on the crime scene. After the arrest, in 2018, DeAngelo pleaded guilty to 13 counts of first degree murders in June 2020.

3.2. Forensic genetic genealogy as an "outgrowth" of the familial searching technique: a way to step over safeguards regulating traditional DNA analysis?

The great mediatic attention dedicated to this case, together with the profound debate it spurred on privacy, ethical, societal and legal concerns deriving from the employment of commercial third-party genealogical databases for investigative purposes, impose a serious analysis of the risks and perils connected to a possible future implementation and extensive use of this technique. Even if some of these issues are similar to the ones already underlined with regards to the *familial searching* instrument, the *forensic genetic genealogy* brings new and additional challenges, due to the peculiar nature, extension and data retained in the recreational databases searched by law enforcement authorities.

In this regard, *forensic genetic genealogy* can be considered an "outgrowth"[50] of familial searching of government-run criminal DNA databases but, differently from the latter, the former technique offers expanded potentialities – and dangers –: while a familial search in the NDIS repository can identify, at best, siblings, parents or children related to the offender's DNA profile, the application of genetic genealogy to commercial databases' information can trace thousands of relatives. As a result, "the sheer number of persons who must be investigated, and the amount of information law enforcement must amass on those persons in order to winnow down candidates, far exceeds that of a typical familial search".[51] Although these characteristics – able to detect a significant number of long-distance relatives starting from the unknown offender's genetic profile – represent the strength and the most relevant potential of the *forensic genetic genealogy,*[52] they also unveil the vast intrusiveness of this instrument. Unlike the *familial searching*, which results effective only if the

over his/her DNA. On this well affirmed, yet debated, theory, see more broadly E. JOH, *Reclaiming "abandoned" DNA: the Fourth Amendment and genetic privacy*, in *North Western University Law Review*, 2, 2006, 857-884.

[50] E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e5.

[51] *Ivi*, e6; the author underlined that in the *Golden State Killer* case the investigators "mapped thousands of relatives, creating 25 distinct lines on the family tree"; in addition, during the investigations "at least two persons had their DNA sampled as a result of false leads in the database", and other genealogical databases have been searched (Ysearch for example) together with GEDmatch; these searches also led to an innocent 73-years-old man, living in Oregon, who was wrongfully identified and searched, being totally unrelated to the case. These exemplifications contribute to deeply understand the vast amount of individuals that can be subjected to investigations and searches thanks to the use of *forensic genetic genealogy*.

[52] From a technical point of view, some authors underlined that "even when the only matches are distant and large family trees must be constructed because common ancestors are many generations in the past, genetic genealogists can triangulate among the matches to determine the most promising branches of the family tree [...]. Even for perpetrators who are completely under the radar or long dead, given DNA from a crime scene, it may be possible to identify them with genetic genealogy [...]. Looking to the future, genetic genealogy has the potential to significantly reduce the number of unsolved cold cases in North America while also reducing the rate at which cases go cold", E. M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit., 113.

unknown offender has relatives already sentenced for a crime,[53] in the *forensic genetic genealogy* technique people whose DNA profile is compared to the unknown offender's one are individuals – not necessarily connected or related to a convicted person – who decided to upload their genetic information only for medical testing or ancestry detection. In addition, it should be considered that "individuals are often aware of even distant family members' arrests. This is especially true for violent or serious crimes, when police can take DNA at the time of arrest. By contrast, a person may not know that an immediate family member sent a DNA sample to a company for medical testing or ancestry analysis"[54] and consequently cannot know in advance to what extent his/her privacy is exposed because of a – even distant – relative's decision to upload the genetic profile in a private genealogy repository.

From all these considerations, it is clear that genetic genealogy as investigative tool entails a much more profound impact in terms of number of people involved, potentially subjecting thousands of innocent users to investigations, without any reasonable suspect justifying or explaining such an invasive intrusion into the private sphere. While the policies and rules regulating *familial searching* in certain States, as seen in Paragraph 2, have been adopted to limit the impact of generic and suspicionless genetic searching, genealogic databases' searches seem to be, at the moment, exempted from these strict conditions. The use by public authorities of what has been called a "fishing expedition-approach",[55] can lead police to "sneak sampling persons in the family tree [determined through the use of the genealogy database information] even though they are not suspects, simply because such samples might help expedite the investigation by eliminating potential suspect branches".[56] What emerges is the potential capability of this instrument to bypass and step over the safeguards ruling traditional DNA searches, motivated by the need to minimize the amount of sensitive data retained by law enforcement authorities in publicly run databases. Considering the great involvement of mainly innocent individuals, together with the lack of rules and regulatory oversight that characterizes this new technique, the main risk is that *forensic genetic genealogy* could be used to circumvent fundamental principles such as the presumption of innocence, freedom from unreasonable search and seizures and ban of unlimited and bulk surveillance and control.[57]

---

[53] Considering the *Golden State Killer* case, it is worth mentioning that DeAngelo"s brother was convicted in California: nonetheless, his DNA profile was not collected and retained in a police-held criminal database, as his crime and conviction occurred before the Proposition 69 of California (which imposes mandatory collection and retention of DNA profile from all felons) entered into force. It is clear that if the genetic profile of DeAngelo"s brother had been uploaded in the criminal DNA database, the *familial searching* technique alone would have been successful in detecting the existent relationship between the unknown offender and his brother. But, as underlined before, the *familial searching* in criminal databases can properly work only if a genetic profile belonging to a close relative of the unidentified offender is retained. On this point, see more broadly, D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 114.

[54] H. L. KODY, *Standing to challenge familial searching of commercial DNA databases*, in *William & Mary Law Review*, 1, 2019, 317.

[55] D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, cit., 203.

[56] E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e7.

[57] "While familial searching in forensic DNA databases is framed by a series of inclusion and exclusion criteria that impose some safeguards in terms of genetic privacy, private companies have extensive databases, with few restrictions and inexistent governance. Long range familial searches in recreational DNA databases thus

3.3. The Privacy Policies established by commercial genealogy companies and the limits of the "informed consent"

In the specific US context, where this technique has firstly been used and implemented, some scholars pointed out the worst but still possible scenario: "it does not take special insight to see that law enforcement is likely to turn to genealogical databases not just to find matches in cold cases that fail to return hits in the forensic databases, but also in situations where federal or state laws expressly forbid such searches for quality control or privacy reasons".[58]

These serious concerns are strictly linked to some specific features of the *forensic genetic genealogy*. First of all, the absence – at least at the moment – of peculiar and dedicated policies and safeguards disciplining the use of this instrument is accompanied by a lack of transparency on its implementation by law enforcement authorities: in the *Golden State Killer* case, for example, only few details were initially shared by investigators about the use of genealogical databases and on the conditions and procedures followed to obtain access to data retained in these repositories. This consequently leads to a second legal as well as ethical issue: can the police upload of the unknown offender's DNA profile be considered in compliance with the privacy policy of the commercial genealogy database? And what about the "informed consent" given by the genealogy services' users? Was the possible access and search for law enforcement purposes clearly accepted by consumers? The answer to these questions entails complex considerations: the genealogy company 23andMe, in a specific "Guide for Law Enforcement" published on the company website in 2018, clearly defined a violation of its terms of service "for law enforcement officials to submit samples on behalf of a prisoner or someone in state custody who has been charged with a crime".[59] This company, similarly to MyHeritage or AncestryDNA, firmly opposes to law enforcement exploitation of its databases, unless a court order or search warrant is provided.[60]

On the contrary, GEDmatch updated its "Terms of Service and Privacy Policy" in 2018, soon after the *Golden State Killer* case became publicly debated: the company openly and clearly allows law enforcement authorities to access the database, by specifying to consumers that "while the results presented on this Site are intended solely for genealogical research, we are unable to guarantee that users will not find other uses, including both current and new genealogical and non-genealogical uses. For example, some of these possible uses of Raw Data, personal information, and/or Genealogy Data by any registered user of GEDmatch include [...] familial searching by third parties such as law

offer a way of circumventing long-established protocols in forensic DNA databases", H. MACHADO, R. GRANJA *Forensic genetics in the governance of crime*, cit., 94.

[58] E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e7.

[59] See 23andMe website at https://www.23andme.com/law-enforcement-guide/.

[60] "23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access. In certain circumstances, however, 23andMe may be required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information", in https://www.23andme.com/law-enforcement-guide/; 23andMe and AncestryDNA also publish reports communicating the amount of access-requests received and granted to law enforcement authorities for investigative purposes.

enforcement agencies to identify the perpetrator of a crime, or to identify remains".[61] Similarly and interestingly, also FamilyTreeDNA (FTDNA) declared in 2019 that "they were collaborating with the FBI and allowing them to upload DNA profiles and create accounts with the same level of access as ordinary users. Existing customers could choose to opt out of matching but this would mean that they would not benefit from the services they had paid for. It was later revealed that the FBI had already been accessing the FTDNA database for an undetermined time without the company's knowledge".[62]

Notwithstanding the different reactions of private commercial databases, reflecting the divergent positions also characterizing the civil society opinion,[63] what clearly appears as a profound and still unsolved issue is the lack of "guarantee that data shared by users actually belong to them".[64] In other words, it is difficult to imagine a way in which commercial genealogy companies could concretely enforce their positions and policies on investigators' access to their databases and assess that no violations are put in place – especially if law enforcement authorities, as happened in the *Golden State Killer* case, don't declare their identity and intentions.

Considering these weaknesses and although companies' Privacy Policies and Terms and Conditions have been, in some cases,[65] changed in order to better inform consumers, also the users' consent

[61] See the GEDMatch website at: https://www.gedmatch.com/tos.htm.

[62] D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 112.

[63] On this point, Kennet recalls that "a survey of 1587 US residents over the age of 18 found that the majority of respondents supported the police use of genealogy databases to identify perpetrators of violent crimes, perpetrators of crimes against children, and missing persons. The majority of respondents were not in favourof such usage to identify perpetrators of non-violent crimes. Since then, genetic genealogy databases have been used to identify the mothers of two abandoned babies and some people consider this is a step too far", D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 112. Also Greytak underlined that "the public is strongly in favor of the use of genetic genealogy to investigate violent crimes: GEDmatch saw a significant increase in the number of participants after the Golden State Killer arrest, and a recent survey showed overwhelming public support", E. M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit., 107. On the contrary, some authors expressed doubts on the reliability of surveys related to the public acceptance of *forensic genetic genealogy*: "as more people become familiar with the vulnerabilities of personal genetic services, opinions may shift regarding the acceptability of police access to data that are generated by and shared with these services. [...] While perceived invasions of privacy appear to be tolerable when the purpose is to catch violent or particularly depraved offenders, it seems that many would draw a line at searching their data to solve more ordinary crimes", 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*, 20, 2018, 8. See also H. MACHADO, R. GRANJA *Forensic genetics in the governance of crime*, cit.

[64] C. GUERRINI, J. ROBINSON, D. PETERSEN, A. 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*, 10, 2018, 7.

[65] It is worth underlining that "an international review of 22 companies" and databases" policies showed that only four companies have provided additional information on how law enforcement agencies should request permission to use their services for law enforcement purposes. Two of these companies were GEDMatch and FamilyTreeDNA, two companies that permit investigative genetic genealogy – and these companies have each taken a different approach to consent. Both databases do not allow specific case-by-case consent, but rather ask for broad consent, though – more in line with dynamic consent – with the option of flexibly changing the consent settings at any time", G. SAMUEL, D. KENNET, *Problematising consent: searching genetic genealogy*

implies challenging aspects: "consumers of genealogy tests now have to confront the tension between the need to protect their own privacy and that of their close and distant relatives, and their strong desire to use this information for their own genealogical research. It is for them to choose between the two, but they need to do so on an informed basis"[66] In order to give a truly informed consent, users should be clearly made aware that their decisions "to contribute their own genetic information inadvertently exposes many other across their family tree who may not be aware of or interested in their generic relationships going public".[67] Differently from the *familial searching* of national DNA databases, which implies that no free consent has been given by convicted criminals or arrestees – whose DNA profile is mandatorily included in the police-held database –, the choice to upload a genetic profile to a genealogy services' website is voluntary but, in this specific case, not strictly "personal" because of the effects and "indirect" involvement produced over – even distant and mainly unaware – relatives.[68]

Following these considerations, some scholars started talking about "generational consent", as a new form of consent including "more than just the individual in decisions about participating in genetic investigations".[69]

This dynamic and still open debate on privacy and data protection concerns linked to the development of genetic genealogy investigations, highlights how this new technique imposes a serious reconsideration and re-thinking of the "traditional" idea of consent. If this instrument is still recognized of key importance, especially in contexts, such as the US one, where privacy and data protection legislations are not fully in place,[70] the peculiarities and specific challenges posed by

databases for law enforcement purposes, in *New Genetics and Society*, 2020, https://bit.ly/3dFvebx, 5, recalling a survey of S. SKEVA, M. LARMUSEAU, M. SHABANI, *Review of policies of companies and databases regarding access to customers" genealogy data for law enforcement purposes*, in *Personalized Medice*, 2, 2020, 141-153.

[66] D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, cit., 204.

[67] S.M. FULLERTON, R. ROHLFS, *Should police detectives have unrestricted access to public genetic databases?*, in *Leapsmag*, 23 July 2018.

[68] Dangers are even more profound if we consider how difficult it is for consumers to fully understand and properly evaluate the risks for their privacy and data when reading usually complex services" privacy policies (especially if online): a truly informed and free consent should be promoted though transparent, clear and easy terms and conditions, giving the consumer a concrete idea of the perils and possible side effects deriving from his/her approval. Moreover, it should be properly considered that "consumers have a tendency towards inertia, particularly when decisions are complex, meaning that they are unlikely to change their opt-in preferences related to consent on the website", G. SAMUEL, D. KENNET, *Problematising consent: searching genetic genealogy databases for law enforcement purposes*, in *New Genetics and Society*, 2020, https://doi.org/10.1080/14636778.2020.1843149, 5. This point underlines the problems and weaknesses related to the use of "opt-out" policies.

[69] "Traditional informed consent reflects individualistic decision-making. We argue that it is time to think of consent in broader terms, as a discussion that, when involving genetic information, goes beyond the individual and asks all parties to think about and involve the broader family and biological relatives", S.E. WALLACE, E. GOURNA, V. NIKOLOVA, N. SHEEHAN, *Family tree and ancestry inference: is there a need for a "generational consent"?*, in *BMC Medical Ethics*, 16, 2015, https://doi.org/10.1186/s12910-015-0080-2.

[70] In US, the use of genetic data and genetic privacy are regulated by two federal laws: the Health Insurance Portability and Accountability Act of 1966 (HIPAA) and the Genetic Information Non-discrimination Act of 2008 (GINA). Some States have approved general data protection laws, providing safeguards also to sensitive data, such as genetic and biometric data or have adopted specific provisions disciplining "genetic privacy". A federal general legislative framework regulating data protection, similarly to the EU Regulation 2016/679, is not in

genealogy forensic must be carefully taken into account: the "traditional" individualistic dimension of consent less suits the privacy issues related to genealogy databases.[71]

All the challenges identified in this paragraph provide a clear picture of the complex concerns and challenges highlighted by lawyers, academics, civil society, geneticists and law enforcement authorities: the still open and unanswered doubts and questions – concerning potentialities, efficiency,[72] side effects and risks, privacy, safeguards and limits to be put in place – call for a profound discussion able to result in a clear and crucial intervention of legislators and policymakers.

4. How to avoid "genetic surveillance": paving the path towards a profound guarantee of "genetic privacy"

4.1. The risks of a "universal database": some timid attempts of regulatory answers

The critiques and the serious ethical and legal concerns emerged in the aftermath of the *Golden State Killer* case have not prevented US law enforcement authorities to solve many other cold or active cases thanks to *forensic genetic genealogy.*[73] This tendency seems to confirm that, "far from being a forensic anomaly, the public genetic search is quickly on its way to becoming routine procedure".[74]

---

place. On the gaps of the existent legislative discipline and the problematic approach adopted by some federal and State Courts, see R.M. HENDRICKS-STURRUP, A. PRINCE, *Direct-to-consumer genetic testing and potential loopholes in protecting consumer privacy and non discrimination*, in *JAMA*, 19, 2019, 1869 ff.; S. LUND, *Ethical implications of forensic genealogy in criminal cases*, in *The Journal of Business, Entrepreneurship & the Law*, 2, 2020, 203 ff.

[71] See also N. SCUDDER, *Privacy and the search for suspects using forensic genetic genealogy*, in *Privacy Law Bulletin*, 5, 2020, 78-81; more generally on consent, A.M. FROOMKIN, *Big Data: destroyer of informed consent*, in *Yale Journal of Health Policy, Law and Ethics*, 3, 2019, 30-54.

[72] "While the commercial autosomal DNA relative-matching tests have essentially been validated by usage by millions of genealogists, the methodologies have not been validated for forensic use. Forensic samples are likely to be degraded, producing a large a number of no calls, and it is not known what impact this will have on the relationship predictions. The proprietary techniques used by Parabon, the DNA Doe Project and the other companies are still experimental and have not been subjected to peer review, creating concerns about transparency and accountability", D. KENNET, *Using genetic genealogy databases in missing persons cases and to develop suspect leads in violent crimes*, cit., 109.

[73] On this point, see H. MACHADO, R. GRANJA *Forensic genetics in the governance of crime*, cit., who also recall Y. ERLICH, T. SHOR, I. PE"ER, S. CARMI, *Identity inference of genomics data using long-range familial searches*, in *Science*, 6415, 690-694; but also E.M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit.

[74] 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*, cit., 9. Doubts on a possible extensive employment of this techniques were initially expressed by some scholars, mainly because of the elevate costs required in terms of time, money and human resources (see E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e7.) Nonetheless, technological and scientific advancements (such as in the field of algorithms and AI instruments) could make the implementation of this instrument more and more easier in the future.

Similar to what happened with regards to the *familial searching* technique and although DNA searches of third-party databases remain mainly an "uncharted" territory, in recent years we are witnessing some first timid attempts to discipline the use of forensic genealogy.

In January 2019 the US Department of Justice approved an interim policy,[75] establishing useful guidelines and case-criteria: "investigative agencies may initiate the process of considering the use of forensic genetic genealogy searches (FGGS) when a case involves an unsolved violent crime (homicide, sex crime) and the candidate forensic sample is from a putative perpetrator, or when a case involves what is reasonably believed by investigators to be the unidentified remains of a suspected homicide victim. In addition, the prosecutor may authorize the investigative use of FGGS other than violent crimes [...] when the circumstances surrounding the criminal act(s) present a substantial and ongoing threat to public safety or national security. Before an investigative agency may attempt to use FGGS, the forensic profile derived from the candidate forensic sample must have been uploaded to CODIS and subsequent CODIS searches must have failed to produce a probative and confirmed DNA match" (point V); the prosecutor should assess that the genealogy forensic is a necessary and appropriate step to develop investigative leads at that stage of the investigation (point VII). Specific rules on the relationship between investigators and genealogy services and databases are established, providing that "investigative agencies shall identify themselves as law enforcement to genetic genealogy services and enter and search profiles only in those services that provide explicit notice to their service users and the public that law enforcement may use their service sites to investigate crime or identify unidentified human remains" (point VII).

By determining limits and rules, these guidelines certainly go in the direction of stronger restrictions and comprehensive safeguards; nonetheless the interim policy still "have room for improvement and still leave the door open for troubling privacy violations":[76] the provisions apply only to the Department of Justice agencies – so that State and local law enforcement authorities are excluded from the scope of application of this document – and the numerous exceptions risk to legitimize discretionary decisions. Terms such as "threat to public safety or national security", allowing for *forensics genealogy* out of the specific serious crimes' cases listed in the policy, could be extensively interpreted and applied. The "explicit notice" law enforcement agencies are required to give to private genealogy databases is an important safeguard, prohibiting what already happened in the past (the upload of a DNA profile by investigators without disclosure of their status and their purposes). But this doesn't guarantee a complete users' protection: the unclear and often not-understandable privacy conditions provided by the genealogy services don't allow for a fully informed consent of the consumer; on the contrary, requiring "an opt-in approach, whereby law enforcement only receives access when a user actively gives permission, would ensure that users approve the site's policy"[77] or the changes applied over the time.[78] Furthermore, no obligation to

[75] Available at https://www.justice.gov/olp/page/1204386/download.

[76] J. SCHWAB, *New DOJ policy gives genealogy website users weak privacy protections from law enforcement*, in *Harvard Civil Rights – Civil Liberties Law Review*, 3 October 2019, https://harvardcrcl.org/new-doj-policy-gives-genealogy-website-users-weak-privacy-protections-from-law-enforcement/.

[77] J. SCHWAB, *New DOJ policy gives genealogy website users weak privacy protections from law enforcement*, cit.

ISSN 2284-4503

notify affected users is specified in the approved guidelines nor a warrant, based on probable cause, is requested; the policy doesn't even answer the privacy concerns linked to the "individual" nature of the consent and to the consequent need to protect not only the consenting user but also his/her relatives. Consequently, if this interim policy is a first meritorious attempt to address the challenges posed by this new investigative tool, it should nonetheless leave space for a profound and comprehensive revision, able to re-consider all the problematic legal and ethical aspects emerged from the public debate.[79]

The evolution of the *forensic genetic genealogy* in the US is carefully followed also in Europe: in September 2020 the UK Government published a Report of the Biometrics and Forensics Ethic Group,[80] focusing on the feasibility of such technique in the UK context. In the conclusions provided by the advisory group a very cautious approach emerges: "the legality and necessity of police use of genetic genealogy in the UK would need to be clearly established with reference to Art. 8 ECHR and the Human Rights Act 1988. The approach should be used if it can be shown to be based on clear evidence, verified by an independent body, that the established methods already in use for these law enforcement purposes are no longer adequate or effective. Otherwise, the use of any such novel processes would not meet the tests of necessity and proportionality. This would make the legality of using such novel processes highly suspect. [...] Legislation for the transmission, length of retention, and destruction of the sample, profile and collected genealogical data would be needed".[81] In requiring prior and comprehensive rules and safeguards, the Group seems to question the legitimacy and the concrete utility of this technique in UK, also underlining that "UK already has one of the most efficient DNA databases in the world and conventional methods, with appropriately applied familial searches, will identify the bulk of perpetrators".[82]

---

[78] In this sense, it is worth noting that in May 2019 "GEDmatch revised its policy to an active "opt in", where consumers had to actively agree to be included in any searches done by government agencies", S. LUND, *Ethical implications of forensic genealogy in criminal cases*, cit., 202.

[79] S. LUND, *Ethical implications of forensic genealogy in criminal cases*, cit., 207, recalling P. ST. JOHN, *DNA genealogical databases are a gold mine for police, but with few rules and little transparency*, in *Los Angeles Times*, 24 November 2019, https://www.latimes.com/california/story/2019-11-24/law-enforcement-dnacrime-cases-privacy .

[80] "The Biometrics and Forensics Ethic Group is an advisory group non-departmental public body, sponsored by the UK Home Office. The group provides advice on ethical issues in the use of biometric and forensic identification techniques such as DNA, fingerprints, and facial recognition technology", https://www.gov.uk/government/publications/use-of-genetic-genealogy-techniques-to-assist-with-solving-crimes/should-we-be-making-use-of-genetic-genealogy-to-assist-in-solving-crime-a-report-on-the-feasibility-of-such-methods-in-the-uk-accessible-version.

[81] See the Report at https://www.gov.uk/government/publications/use-of-genetic-genealogy-techniques-to-assist-with-solving-crimes/should-we-be-making-use-of-genetic-genealogy-to-assist-in-solving-crime-a-report-on-the-feasibility-of-such-methods-in-the-uk-accessible-version.

[82] Notwithstanding the open debate, some authors have already highlighted that "a small convenience sample pilot study has already demonstrated the method would work in the UK setting", G. SAMUEL, D. KENNET, *Problematising consent: searching genetic genealogy databases for law enforcement purposes*, in *New Genetics and Society*, 2020, https://doi.org/10.1080/14636778.2020.1843149, 3; see also J. THOMSON, *An empirical investigation into the effectiveness of genetic genealogy to identify individuals in the UK*, in *Forensic Science International: Genetics*.

Regardless of the different possible views and approaches, what seems to be uncontroversial is, on the one side, an increasing tension towards an extensive use of DNA analysis in the law enforcement field and, on the other side, a growing awareness of the serious challenges deriving from these techniques.[83]

4.2. How to resist the temptation of "seeing into the life of citizens": prompting a thoughtful and pondered debate

Even if not always totally or *per se* decisive,[84] the development of new forensic DNA techniques has enabled "a new wave of crime-solving technology",[85] with particularly positive effects on the capability to solve cold cases, when all the other possibilities revealed a dead end. As Syndercombe Court underlined, the *familial searching* of DNA criminal databases has been considered, since the beginning, "a 'quantum leap' in forensic identification, and is made even more significant today by the use of genealogical databases".[86] Both these investigative tools move "the locus from individualization, that is, identification of specific individuals, towards collectivization [...], by clustering 'suspect' populations which share biological links and genetic ancestry".[87] By doing so, these innovative instruments have been extensively criticized for their capability to expose innocent people to life-long surveillance[88], to exacerbate already existent racial inequalities and discriminations and to consequently debunk 'genetic privacy' safeguards. What is feared the most is the possible detrimental shift to "a *de facto* universal database", especially through the use of genealogy connections:[89] this will conduct to a significant expansion of "the scope and impact of genetic surveillance",[90] by "constructing suspicion as collective".[91] The use of private companies'

[83] In 2008, the ECtHR, in the already recalled *S and Marper v. UK* decision, recognized the dangerous tendency to allow "modern science techniques in the criminal-justice system [...] at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private life interests", para. 112.

[84] Using these research methods does not always assure a result: "while there certainly will be more announcements of cases solved using this new technique, there are many more cases where identification has not yet been possible, due to the wide variety of complications present in these investigations", E. M. GREYTAK, C. MOORE, S. L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit., 103.

[85] R. WICKENHEISER, *Forensic genealogical searching and the Golden State serial killer*, in *Forensic Science International*, 1, 2019, S9.

[86] D. SYNDERCOMBE COURT, *Forensic genealogy: some serious concerns*, cit., 204, recalling E. MUPRHY, *Relative doubt: familial searches of a DNA database*, in *Michigan Law Review*, 109, 2010, 291-348.

[87] H. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, cit., 86.

[88] S. KRISMKY, T. SIMONCELLI, *Genetic justice: DNA data banks, criminal investigations and civil liberties,* New York, 2011.

[89] E. MURPHY, *Law and policy oversight of familial searches in recreational genealogy databases*, cit., e7. According to the author, "essentially everyone will be a police database now". Expressing a pessimistic view, Murphy forecasts that "the prevalence of genealogical DNA databases searches will begin to infect the debate about the use of governmental databases, and prompt the loosening of existing regulations rather than the enhancement of the regulatory architecture for genealogical searches", e7.

[90] A similar expression was significantly used by Justice Scalia in his Dissenting Opinion in the abovementioned *Maryland v. King* decision (*supra* note 11): in that case – concerning the possibility to collect DNA samples from arrestees – Justice Scalia warned against the perils of a "genetic panopticon", para. 1900.

[91] C. MACHADO, R. GRANJA, *Forensic genetics in the governance of crime*, cit., 92 and 99.

databases, less regulated and controlled compared to national and publicly-led databases, brings an additional layer of complexity.[92]

The seriousness of the underlined risks and the rapidly increasing use of sophisticated but highly intrusive investigative techniques, mainly in the absence of specific regulatory frameworks, prompts for a thoughtful and pondered legislative discussion, before these instruments become widely applied. Accordingly, a comprehensive set of rules should be determined, on the basis of a careful risk-assessment: with regards to *forensic genetic genealogy*, "there must be a process to ensure genealogical searching is conducted properly scientifically and from a public policy perspective. There should be transparency of policies, procedures and documentation to guide and demonstrate appropriate use".[93] A dedicated training of law enforcement authorities, illustrating a proper and correct application of the new techniques, should be followed by an exhaustive discipline of privately-run genealogy services, also strengthening the effectiveness of a truly informed consent on the consumers' side: it can be, for example, imposed to genealogy companies and databases to clearly and unambiguously inform users about the risk to expose their genetic privacy and that of their relatives to the access of law enforcement agencies for investigative purposes, extensively explained and priorly determined. Company reports on the factual access by investigators should be a recommended practice. Moreover, specific policies and laws should be approved in order to establish precise limits to the employment of both *familial searching* and *forensic genetic genealogy*: determining what kind of crimes could allow for familial or genealogy searching in private databases, or what kind of requests should law enforcement authorities present, in a transparent way, to the genealogy companies, are of paramount importance to set well-defined safeguards able to minimize abuses and avoid an extensive recourse to invasive techniques, which should be considered the last possible resort. The conditions that justify the implementation of these investigative tools, virtually capable of targeting a vast number of innocent people, should be determined according to the principle of proportionality, necessity and data minimization. These considerations should inspire and guide legislators and policymakers to rapidly move towards efficient and comprehensive regulatory answers.

---

[92] Divergent points of view are expressed on this difficult topic: some authors consider that if a person, based on correct information, voluntarily decides to upload his/her DNA profile on a genealogy website, there are no reasons to prevent police from employing these data (E. M. GREYTAK, C. MOORE, S.L. ARMENTROUT, *Genetic genealogy for cold case and active investigations*, cit.). On the contrary, Kody affirms that "allowing a company to analyse one"s DNA for medical or ancestry purposes does not do away with the protection all Americans have to be free from unreasonable and unwarranted government intrusion", L. KODY, *Standing to challenge familial searching of commercial DNA databases*, cit., 318.

[93] R. WICKENHEISER, *Forensic genealogy, bioethics and the Golden State Killer case*, cit., 123. Similarly, Berkman, Miller and Grady affirmed that "a commitment to transparency is extremely important. Authorities apparently are reluctant to admit that they use forensic DNA searching, despite the fact that most states do so. If law enforcement is using this technology, the adoption of formalized standards and mechanisms of accountability is appropriate. The limits of DNA evidence also suggest that restrictions should be placed on its use. We recommend using forensic genealogy as an investigative tool rather than a primary source of evidence of criminal wrongdoing. Likewise, justice concerns might warrant limiting criminal genealogy searching to cold cases involving crimes in which other investigative methods have failed", B. BERKMAN, W. MILLER, C. GRADY, *Is it ethical to use genealogy data to solve crimes*, in *Annals of Internal Medicine*, 5, 2018, 334.

In this context, the question that should be posed at the very basis of every consideration and decision should be "to what extent can the rights of the innocent general public and relatives of the committer of a crime be infringed upon by examining their genetic data to identify the crime perpetrator and thereby prevent future crimes and improve public safety?".[94] Although addressing this question and determining a correct balance-point will probably be imperfect and non-final,[95] the necessary answers cannot be left to the consent of users or to the privacy policies set by private companies, and should, on the contrary, be properly managed by public policies and laws.

In conclusion, the rising implementation of *familial searching* and *genetic genealogy* forensics exemplify the diffuse public authorities' desire to fully exploit the potentialities of very sensitive and personal data together with the opportunities represented by new technological tools or procedures. The tendency to collect, retain, access and employ a great amount of data for the sake of security or efficiency of public services is visible in many other fields, from the mandatory retention of telecommunications' metadata for public and national security purposes to facial recognition technologies as crime-fighting tool, from biometric identification systems necessary to access fundamental welfare services, to automated risk management tools used to detect tax and welfare frauds:[96] these trends draw a dangerous shift towards over-surveillance and the creation of societies in which citizens are subjects to control and intrusion in their more intimate sphere, also through the use of very unique and sensitive data.

As former ECtHR Judge Pettiti clearly stated, back in the 1980s, "the danger threatening democratic societies [...] stems from the temptation facing public authorities to see into the life of citizens".[97] This widespread temptation – fuelled by the increasing "datification", digitalization and technological progress and possibly able to undermine, at their very basis, fundamental rights' guarantees and safeguards – must be seriously and rapidly tackled, in all its expressions, by civil society, scholars, legislators and Courts. This paper's ambition – and hope – is to help keep such a vital debate alive.

---

[94] R. WICKENHEISER, *Forensic genealogical searching and the Golden State serial killer*, cit., S9.

[95] As brilliantly stated by Suter, with regards to *familial searching*, "in some ways the conflict seems insoluble. Proponents and opponents of familial searching [but the same is true for genetic genealogy forensic] are both fighting the "good fight". Both are motivated by defensive postures. Proponents want to fight crime; opponents want to fight violations of civil liberties. When each side is so deeply passionate about its underlying goals, it becomes difficult not only to find a compromise, but even to agree upon a common approach to resolving this and other difficult dilemmas. In short we face the challenge of there being a plurality of important values, some of which collide. How do we handle this collision and the possibility that some of the values may have to give away in certain contexts?", S. SUTER, *All in the family: privacy and DNA familial searching*, cit., 375.

[96] See for example the legal challenges emerged from the "data retention regime" in the EU as well as the long and complex ECJ "data retention saga"; see also the controversial use of Syri: this program, adopted in the Netherlands and aimed at detecting tax frauds through the automated analysis of data collected and retained by public agencies, was declared unlawful by the District Court of the Hague because of its lack of transparency and disproportionate interference with citizens" private life. The debate is still open in Ireland and France for the adoption of automated biometric identification systems aiming at granting citizens" access to public welfare services; similarly, the use of facial recognition for law enforcement purposes, based on the collection and comparison of sensitive data belonging to mainly innocent citizens, has been challenged before UK Courts.

[97] ECtHR (2 August 1984), *Malone v. UK*, n. 8691/79, Judge Pettiti Concurring Opinion, para. 38.

ISSN 2284-4503