A new approach to the right to privacy, or how the European Court of Human Rights embraced republicanism

As it is currently regulated, the right to privacy is predominantly conceived as a subjective right protecting the individual interests of natural persons. In order to determine whether this right has been affected in a specific situation, the so-called 'non-interference' principle is applied. Using this liberal concept, it follows that the right to privacy is undermined if an 'infringement' with that right by a third party can be demonstrated. Although the 'infringement'-criterion works well when applied to more traditional privacy violations, such as a third party entering the home of an individual or eavesdropping on a private conversation, with respect to modern data-driven technologies, it is often very difficult to demonstrate an actual and concrete 'infringement' on a person's right or freedom. Therefore, an increasing number of privacy scholars advocates the use of another principle, namely the republican idea of 'non-domination'. At the core of this principle is not the question of whether there has been an 'interference' with a right; rather, it looks at existing power relations and the potential for the abuse of power. Interestingly, in recent times, the European Court of Human Rights seems to accept the republican approach to privacy when it deals with complex data-driven cases.

1. Introduction

New technological developments, such as Big Data, cloud computer and the internet of things, put our current understanding of and the regulatory approach to privacy protection under pressure. For example, although for centuries, there has been a social and legal divide between the private and the public domain, both spheres are becoming increasingly blurry. Smart devices are entering the home and with them the control of third parties over what we do in our homes.[1] Conversely, the public sphere is becoming more and more hybrid. Private life and private objects are increasingly located in this space, for example the smart phone, iPad or laptop.[2] Many of the current legal systems lay down safeguards against the police entering the home of an individual, but very few safeguards for entering a smartphone, while for most people, this is considered a major privacy interference.[3] To provide another example, although the freedom of correspondence and the privacy of communications are protected through legal means, more and more, scholars argue that meta-data about such correspondence should also be provided protection. Seeing recent legal developments through which the police and other governmental authorities are vested with the power to hack computes and other devices, scholars have argued that not only communications should be protected, but the integrity of personal devices as well.[4] And then there are debates about whether 'personal data' is still a useful concept in the age of Big Data, because in fact all 'data' can be used to make choices that have a high impact on society and the people living

[1] R. van den Hoven van Genderen, 'Privacy and Data Protection in the Age of AI and Robotics', European Data Protection Law Review, 2017-3.
[2] See also: Supreme Court Riley v. California, 573 U.S. (2014).
[3] E. J. Koops & M. Galic, 'Conceptualising space and place: Lessons from geography for the debate on privacy in public'. In T. Timan, B. Newell, & E. J. Koops (Eds.), 'Privacy in public space: Conceptual and regulatory challenges', Edward Elgar Publishing, 2017.
[4] See also: BVerfG 27 February 2008.

therein. Shouldn't we regulate 'data' instead of 'personal data'?, is a question that is increasingly posed.[5]

These are more specific challenges for the current approach to the right to privacy catalyzed by technological and societal developments. But there is also a more fundamental question that is becoming ever more urgent. In literature, the right to privacy is primarily approached as the subjective right of a natural person to protect his personal interests, for example related to human dignity,[6] individual autonomy[7] and personal freedom.[8] To determine whether the right to privacy is affected in a certain situation, attention is paid to the question of whether there has been an 'interference' with this right. The use of the so called 'non-interference' principle can be derived from Mill's famous essay On Liberty[9] and the harm principle. 'Non-Interference formalises some of the fundamental insights of the Harm Principle, namely the idea that society should not interfere with individual choices whenever the latter have no (harmful) effect on others. Mill insists that the reasons for the change in circumstances of the individual (such as neglect, irresponsibility, effort or luck) are not relevant information for social judgements, provided that nobody else is negatively affected.'[10] There is only reason to curb a person's freedom if that freedom is used to interfere with another's person's freedom. Vice versa, an inference of the rights or interests of an individual is only found in this liberal understanding of the right to privacy if there has been a specific and concrete interference, resulting in actual harm.

This liberal approach to the right to privacy is embraced in most jurisdictions in the western world, an example of which may be the case law of the European Court of Human Rights (ECtHR) on Article 8 of the European Convention on Human Rights (ECHR), providing: '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'[11] In its dominant case law, the ECtHR has interpreted Article 8 ECHR as a doctrine that provides a subjective right to natural persons to protect their private interests. A complaint about the violation of the right to privacy will only be declared admissible by the Court when the applicant can produce evidence of a concrete and actual 'interference' with this right, which resulted in concrete and actual harm.

Interestingly, both in literature and in the jurisprudence of the European Court of Human Rights, a new approach is increasingly proposed, in which the focus is not put on the principle of 'interference', but on the principle of 'domination'. This republican concept does not assess human rights questions on the basis of whether there has been an actual interference, resulting in harm, but whether there is a position of dependence and whether power can be used in an arbitrary way. This article discusses the right to privacy, technological developments and the leading jurisprudence of the ECtHR. Section 2 briefly

---

[5] See also the new proposal of the European Commission and on that topic: D. Broy, 'The European Commission's Proposal for a Framework for the Free Flow of Non-Personal Data in the EU', European Data Protection Law Review, 2017-3.

[6] B. Roessler, 'The value of privacy', Polity Press, Cambridge, 2005.

[7] S. I. Benn, 'Privacy, Freedom, and Respect for Persons'. In: F. Schoeman (ed.), 'Philosophical Dimensions of Privacy: an Anthology', Cambridge University Press, Cambridge, 1984.

[8] A. F. Westin, 'Privacy and Freedom', The Bodley Head, London, 1970.

[9] J. S. Mill, ''On Liberty' and Other Writings', Cambridge, Cambridge University Press, 1989.

[10] M. Mariottiy & R. Veneziani, 'The Liberal Ethics of Non-Interference and the Pareto Principle', <https://www.st-andrews.ac.uk/~wwwecon/repecfiles/4/1404-ori.pdf>.

[11] Article 8 of the European Convention on Human Rights. <http://www.echr.coe.int/Documents/Convention_Eng.pdf>.

explains how the right to privacy is predominantly approached in literature and case law, which is illustrated by a discussion of the jurisprudence of the European Court of Human Rights. Sections 3 discusses how new data-driven applications challenge this approach, inter alia because it is increasingly hard to demonstrate a concrete 'infringement' and to specify harm. Section 4 discusses several authors that, seeing these problems, have proposed to reduce the importance of the liberal 'non-interference' principle in these kinds of cases and instead focus on the republican 'non-domination' principle. Section 5 shows that rather surprisingly, the ECtHR is prepared to let go of its focus on actual infringements and concrete harm in cases revolving around, inter alia, mass surveillance, instead focusing on non-domination and safeguards against the arbitrary use of power. Section 6 concludes with the potential effect this new position may have on the future of privacy regulation.

2. The right to privacy

Under the European Convention on Human Rights, there are two modes of complaint. Article 33 allows for so called inter-state complaints, in which, for example, Germany can bring a case against France for potential human rights violations. The provision reads: 'Any High Contracting Party may refer to the Court any alleged breach of the provisions of the Convention and the Protocols thereto by another High Contracting Party.'[12] Article 34 allows for so called individual complaints, in which either a natural person, a group of natural persons or a legal person (not being a governmental organization) can bring a complaint about the violation of a human right by a state. The provision reads: 'The Court may receive applications from any person, non-governmental organisation or group of individuals claiming to be the victim of a violation by one of the High Contracting Parties of the rights set forth in the Convention or the Protocols thereto. The High Contracting Parties undertake not to hinder in any way the effective exercise of this right.'[13] Although the intention of the authors of the European Convention on Human Rights was consequently to open up the right to complaint to a number of parties, legal practice has developed differently.

Under the interpretation of the European Court of Human Rights, in principle, only natural persons can complain about a potential violation of the right to privacy. First, the possibility of inter-state complaints has had almost no significance under the Convention's supervisory mechanism. In 2006, when the Court had delivered more than 15.000 judgments,[14] an expert signaled: '[A] total of 19 applications had been lodged by States. Even this very low number provides a distorted picture. In fact only six situations in different States have been put forward in Strasbourg by means of an inter-State application. (…) Given the number of violations that have occurred during the more than 50 years that the Convention has been in force, it is evident that the right of complaint of States has not proved to be a very effective supervisory tool.'[15] With only one inter-state complaint in 2009 and another one in 2011 regarding the same matter, this trend seems to have continued after 2006.[16]

In addition, the Court has rejected the capacity of groups to complain about a violation of human rights. Contrary to the intention of the authors of the Convention, it has stressed that only individuals that have been harmed personally and directly can submit a complaint on their own behalf. At most, different individuals that have all been affected by the same

[12] Article 33 of the European Convention on Human Rights.
[13] Article 34 of the European Convention on Human Rights.
[14] <http://www.echr.coe.int/NR/rdonlyres/E58E405A-71CF-4863-91EE-779C34FD18B2/0/APERCU_19592011_EN.pdf>.
[15] P. van Dijk, F. van Hoof, A. van Rijk & L. Zwaak (eds.), 'Theory and Practice of the European Convention on Human Rights', Intersentia, Antwerpen, 2006, p. 50.
[16] ECtHR, Georgia v. Russia (I), application no. 13255/07, 30 June 2009. ECtHR, Georgia v. Russia (II), application no. 38263/08, 13 December 2011.

violation can bundle their complaints. It is not allowed to submit a complaint on behalf of a group or as a group, such as Gypsies, Muslims or Catalans.[17] And with respect to the right of legal persons to submit an application, the Court has accepted, inter alia, that churches may invoke the freedom of religion (Article 9 ECHR) and that press organizations may rely on the freedom of expression (Article 10 ECHR). However, because Article 8 ECHR, in the interpretation of the ECtHR, only provides protection to individual interests, the Court has stressed that in principle, only natural persons can invoke a right to privacy. For example, when a church complained about a violation of its privacy by the police in relation to criminal proceedings, the Commission found: '[T]he extent to which a non-governmental organization can invoke such a right must be determined in the light of the specific nature of this right. It is true that under Article 9 of the Convention a church is capable of possessing and exercising the right to freedom of religion in its own capacity as a representative of its members and the entire functioning of churches depends on respect for this right. However, unlike Article 9, Article 8 of the Convention has more an individual than a collective character(…).'[18] Accordingly, the Commission declared the complaint inadmissible. This position is still embraced by the Court; it is willing to accept legal persons as complainants only in very exceptional circumstances.[19]

Consequently, Article 8 ECHR has been interpreted by the Court in such a way that it primarily aims at protecting individual interests by granting natural persons a right to complain. The material scope of the right to privacy under the European Convention on Human Rights is also focused on the individual interests of the natural person. While the Convention was originally focused on laying down negative obligations for states (not to abuse their power) and negative rights to citizens (not to be subject of interferences), gradually, the Court has accepted positive obligations for states to actively protect the privacy of citizens and the positive right of citizens to pursue their personality to the fullest, under Article 8 ECHR. This broadly means two things. First, that almost everything that is related to one's personality or life will be considered having an impact on an applicant's 'private life'.[20] Second, while the freedom of expression is linked to personal expression and development, it also connected to the protection of societal interests, such as the search for truth through the market place of ideas and the well-functioning of the press, which the Court holds to be a precondition for every liberal democracy.[21] By contrast, Article 8 ECHR only provides protection to individual interests such as autonomy, dignity and personal development. Cases that do not regard such private matters are in principle rejected by the Court.[22]

This means that in principle, only natural persons can bring a case concerning the right to privacy under the European Convention on Human Rights if the case is directly related to their individual interests. Finally, the Court has stressed that an application will only be declared admissible if it concerns a concrete and direct 'interference' with the right to privacy of the applicant. If the applicant cannot show that there has been such concrete interference with his rights or interests, the application will be declared inadmissible by the European Court of Human Rights. For example, so-called *in abstracto* claims are in principle declared inadmissible. These are claims that regard the mere existence of a law or policy, without them having any concrete or practical effect on the claimant. In the words of the European

[17] Applicants can bundle their complaints if they are the victim of the same interference.
[18] ECmHR, Church of Scientology of Paris v. France, application no. 19509/92, 09 January 1995.
[19] There are a handful of cases in which the Court is willing to relax this point.
[20] See about the widened scope of Article 8 ECHR: B. van der Sloot, 'Privacy as personality right: why the ECtHR's focus on ulterior interests might prove indispensable in the age of Big Data', Utrecht Journal of International and European Law, 2015.
[21] Media-diversity is another classic example.
[22] See for one of the first cases focusing on positive freedom and personal development: ECmHR, X. v. Iceland, application no. 6825/74, 18 May 1976.

Commission on Human Rights: 'Insofar as the applicant complains in general of the legislative situation, the Commission recalls that it must confine itself to an examination of the concrete case before it and may not review the aforesaid law *in abstracto*. The Commission therefore may only examine the applicant's complaints insofar as the system of which he complains has been applied against him.'[23]

A priori claims are rejected as well, as the Court will usually only receive complaints about injury which has already materialized. Claims about future damage will in principle not be considered. 'It can be observed from the terms 'victim' and 'violation' and from the philosophy underlying the obligation to exhaust domestic remedies provided for in Article 26 that in the system for the protection of human rights conceived by the authors of the Convention, the exercise of the right of individual petition cannot be used to prevent a potential violation of the Convention: in theory, the organs designated by Article 19 to ensure the observance of the engagements undertaken by the Contracting Parties in the Convention cannot examine - or, if applicable, find – a violation other than *a posteriori*, once that violation has occurred. Similarly, the award of just satisfaction, i.e. compensation, under Article 50 of the Convention is limited to cases in which the internal law allows only partial reparation to be made, not for the violation itself, but for the consequences of the decision or measure in question which has been held to breach the obligations laid down in the Convention.'[24]

Hypothetical claims regard damage which might have materialized, but about which the claimant is unsure. The Court usually rejects such claims because it is unwilling to provide a ruling on the basis of presumed facts and speculations. The applicant must be able to substantiate his claim with concrete facts, not with beliefs and suppositions. The ECtHR will in principle also not receive an *actio popularis* (sometimes also called class action or collective action), a case brought by a claimant or a collective, not to protect their own interests, but that of others or society as a whole. 'The Court reiterates in that connection that the Convention does not allow an *actio popularis* but requires as a condition for exercise of the right of individual petition that an applicant must be able to claim on arguable grounds that he himself has been a direct or indirect victim of a violation of the Convention resulting from an act or omission which can be attributed to a Contracting State.'[25] Again, the Court requires that the individual bringing the complaint can demonstrate an actual interference with his rights, resulting in concrete harm or damage.

3. Data-driven technologies

The right to privacy is thus primarily linked to the individual, his rights and his interests. The question of whether this right is undermined is primarily judged by the question of whether there has been an 'interference' with this right. This is known as the 'non-interference' principle, which is embraced in most liberal literature and in the legal systems of most western countries. This principle can be derived from the harm principle coined by Mill. Under such an understanding, there is only reason to curb a person's freedom if that freedom is used to interfere with another's person's freedom. The other way around, an inference of the rights or interests of an individual is only found in this liberal understanding of the right to privacy if there has been a specific and concrete interference, resulting in actual harm. This position is also embraced by most courts, as was illustrated by discussing the caw law of the European Court of Human Rights in the previous sections.

[23] ECtHR, Lawlor v. the United Kingdom, application no. 12763/87, 14 July 1988.
[24] ECmHR, Tauira and others v. France, application no. 28204/95, 04 December 1995.
[25] ECtHR, Asselbourg and 78 others and Greenpeace Association-Luxembourg v. Luxembourg, application no. 29121/95, 29 June 1999.

The principle of ‘non-interference’ works relatively well for traditional privacy issues. Although it has always been difficult to materialize and quantify damage - which damage results from entering the home of an individual if no property is stolen and no information about the home communicated to third parties? - it is usually relatively easy to determine an infringement. Most privacy violations are clearly defined in person, time and space. At seven o’clock, the police entered the home of Mr. Brown; from 9 October to 11 November, Mrs. White’s telephone was wiretapped. However, this is different for many modern day privacy issues, often revolving around large data processing operations. These are barely defined in time, space and person and constitute a structural and continuous part of the actions and behavior of government institutions, companies and citizens. As an example, reference can be made to the numerous CCTV-cameras that can be found on the corner of almost every street in some cities. With respect to these types of data-gathering initiatives, the individual is incidental - the cameras do not film a specific person or target a specific group of people. They film everyone, always and anywhere when in sight of the cameras. How can an individual demonstrate that he has been harmed specifically, individually and directly? The same question could be posed with regard to many of the modern data driven technologies.

In addition, a practical problem arises. Assigning individual rights to citizens assumes that they are primarily responsible for the protection of their rights. As discussed, other citizens or civil society organizations cannot, in principle, submit applications on behalf of others, to protect their interests. These class actions are declared inadmissible by the European Court of Human Rights. The difficulty for individuals to claim their rights with respect to large data collection processes is two-fold. On the one hand, a citizen is often unaware of the simple fact that data are collected about him. Citizens make photos and videos of each other on the streets, at parties and elsewhere and post them online, without informing those filmed, let alone asking for their permission. Companies gather large amounts of data using cookies, device fingerprinting and other tools to monitor internet-behavior. Governmental organizations collect substantial quantities of data about citizens, inter alia by using heat sensors, wiretapping and covert surveillance by intelligence agencies. The citizen is usually not informed or aware of these data collection programs. If citizens do not know that their data is collected, they will usually not invoke their right to privacy. On the other hand, there are more and more data flows in which the data of a citizen could be contained. It is virtually impossible for a citizen to check for all of these data flows whether his data is included, who collects the data, whether that is done according to all legal principles and if not, to take the matter to court. Almost everything is data-driven these days; it is impossible for a citizen to assess the legitimacy of all the data processes which may or may not include his data.

More fundamental is the problem that even if the citizen would be aware of all data flows in which his personal data are contained and even if he has the time and the capacity to check for every data processing initiative whether or not it adheres to all legal principles and to go to court if it does not, then it will still be difficult to demonstrate a clear and concrete interference with an individual right. New data-driven technologies generate large amounts of data from all aspects of society. Statistical correlations are detected by using smart algorithms. Group profiles are distilled and translated into policy decisions. With these types of Big Data processes, the individual interest is difficult to substantiate and it is increasingly hard to prove concrete and personal harm following from an interference. For example, the National Security Agency (NSA) has collected data about millions of American and non-American citizens. But what harm has the average American or European citizen suffered from its activities, even though his data may have been gathered by the agency? The larger the data processing initiatives get and the more general the data being processed are, the more difficult it will be for individuals to demonstrate their individual interest and personal harm.

The issue posed by these types of data-driven technologies seems not so much the actual infringement on an individual right, but the power relationship that is created. Due to their possession over increasingly large amounts of data, companies and government organizations gain vast knowledge about the behavior of citizens and the society as a whole. They can use that knowledge to reorganize societal processes or to tacitly influence the behavior of citizens, for example through nudging. Even if they do not use this power or if they use the power only to the benefit of society as a whole and the citizens that are being nudged (for example when they are made less aggressive (for example by spraying tangerine sent in the streets) or nudged towards adopting healthy behavior), the power relationship is still a fact. This is the first problem of modern data processing initiatives, which is not connected to a direct interference or actual harm. The second issue that is also not related to any concrete interference is the *capacity* to use power in an arbitrary way. Those organizations that are involved with large scale data processing initiatives are also the organizations that are often subjected to minimal checks and balances only. A good example are intelligence agencies, which develop mass surveillance programs, but are often exempted from many legal and procedural safeguards that are normally applied under the rule of law. In addition, they are usually subjected to only a minimum form of judicial and parliamentary oversight.[26] The mere fact that a person or organization has power and the mere fact that this power *can* be used freely and arbitrarily implies that citizens can feel themselves curtailed in their freedom and will limit their behavior in anticipations for fear of potential unknown consequences. [27]

4. Republicanism

Because the issues that arises from many modern data technologies revolve only partly around actual and concrete infringements and more and more around power relations as such, scholars have questioned whether the liberal 'non-interference' principle is still relevant in this context. More and more, reference is made to the so-called 'non-domination' principle, as embraced in republicanism and promoted in the work of, among others, Philip Pettit. [28] He argues that liberals traditionally formulate freedom in terms of non-interference, whether viewed as a formal freedom, as most right-wing liberals do, or as a freedom that also implies active involvement by the state, as most left-wing liberals do. Freedom is seen as the freedom from interferences by third parties. Such interference with a person's freedom may consist of, for example, a ban on a demonstration, the prohibition of a particular publication or the breach of the sanctity of someone's home. Liberals, in this sense, look at the concrete and actual state of affairs, rather than at abstract relations and potentials.

The principle of 'non-domination' is not so much focused on concrete violations of rights or freedoms, but looks to power relations as such and the potential for abuse. 'Contrary to Berlin's account of negative liberty - that a person is free to the extent that no other entity actually interferes with that person's activity - Pettit's neorepublican position does away with the requirement of actual interference, focusing on eliminating the danger (or potential danger) of arbitrary interference from others. Rather than predicating freedom on ideas of self-mastery, autonomy, or a person's ability to act in accordance with their higher-order desires, an account of Berlin's positive liberty, neorepublican theory is more concerned with

[26] L. K. Johnson, 'The Oxford Handbook of National Security Intelligence', Oxford University Press, Oxford, 2010.
[27] Also called the chilling effect.
[28] His standard work is: P. Pettit, 'Republicanism: A Theory of Freedom and Government', Oxford, Clarendon Press, 1997.

ensuring the ability of the people to self-govern, by reducing domination and arbitrary interference.'[29]

Pettit himself, in his book *Republicanism,* puts it as follows: '[] advancing someone's freedom as non-domination is likely to help them escape from uncertainty, strategy, and subordination; certainly, it is more likely to do this than advancing their freedom as non-interference. But something stronger also holds true. Suppose we take steps to reduce a person's uncertainty about interference, to reduce their need for exercising a strategy of deference and anticipation with others, and to reduce the subordination associated with vulnerability. It is hard to see how we could take such steps without at the same time advancing their freedom as non-domination. Freedom as non-domination appears to be, not just a more or less sufficient instrument for promoting those effects, but a more or less necessarily associated factor. There is no promoting non-domination without promoting those effects; and there is no promoting those effects without promoting non-domination. This may not hold in every possible world, but it certainly seems to hold under plausible assumptions about how the actual world works.'[30]

A well-known example used to illustrate the distinction between freedom as non-interference and freedom as non-domination is slavery. Liberals as well as republicans will of course reject slavery. If freedom is determined in terms of freedom from interference, it can be said that the exploitation that takes place in this kind of power relations is a clear interference with human dignity and autonomy as well as sexual exploitation, the poor living conditions and the physical violence often part of such power relationships. The lack of freedom of choice and autonomy of the slaves should also be stressed; in the end, the master decides whether what a slave wants to do is actually allowed or not. The slave's autonomy in this sense is often restricted by his master; every time a decision by a slave is limited or overruled by his master, his autonomy is interfered with.

Taking a different perspective, republicanism will focus on the power relationship as such. This relationship is problematic, from this perspective, for two reasons. First, because the power relationship is absolute and second, because there are no safeguards against the arbitrary use of power. A key question raised here is: suppose the master does not use his power in any way – the slaves are fully free to do whatever they like and the master does not pose any restrictions on their desires or actions. What then, from a liberal perspective as freedom as non-interference, would be the problem? There is no interference of any kind. From a republication perspective, this situation is still problematic not because the master interferes with the freedom and autonomy of his slaves, but because he has the power to do so. The core question shifts from the actual use of power to the potential to use the power. In addition, the problem from a republican perspective is that there are no checks and balances against the abuse of power. The master can use his power at any time, in any way that he sees fit. The slave never knows if and when power is exercised over him, so that he will always live in uncertainty and in that sense, will never be fee.

Such questions also play a role in the relationship between citizen and state. Again, republicanism does not look so much to the question of whether the government has actually used its power and whether this has led to a concrete interference, but to the extent of government power and whether sufficient safeguards are in place to prevent the arbitrary use of power. Arbitrary, in this sense, can have both a formal and a material meaning. 'The first defines it procedurally. Power is arbitrary, on this view, to the extent that it is not reliably constrained by effective rules, procedures, or goals that are common knowledge to all persons or groups concerned. To be reliably effective, on this view, constraints must be resilient over

[29] B. C. Newell, 'The Massive Metadata Machine: Liberty, Power, and Secret Mass Surveillance in the U.S. and Europe', 10 ISJLP 481, p. 514-515.
[30] Pettit, p. 90.

a wide range of possible changes or modifications in the relevant circumstances. Roughly speaking, the procedural view equates republican freedom with the traditional idea of the rule of law, provided we are willing to extend the latter idea considerably. Alternatively, we might define arbitrariness substantively: power is arbitrary, on this second view, when it fails to track the "welfare and world-view" of those affected.'[31] The procedural safeguards against arbitrary interference can, inter alia, be specifying when and under what conditions powers can be used. For example, the police may only wiretap an individual upon concrete suspicion of a serious offenses, after having been authorised by a judge. Material arbitrariness lies in the use of power without taking into account the circumstances of the case, the specificities of the persons against whom the power is applied and the context in which the formal competence is exercised. In short, it is about the use of power in a context-blind manner.

In a negative sense, republicanism therefore emphasizes the freedom from relations in which power can be exercised arbitrarily. In this sense, republicans emphasize the classic principles associated with the rule of law, regardless of whether there has been an actual infringement with the right of an individual in a concrete occasion.[32] In positive terms, republicans emphasize the ability of citizens to influence the laws and the state of affairs that apply to them. 'Republican rights are not to be understood as pre-political norms – rights that establish the framework within which political decision making takes place. Rather, they are the product of political decision-making processes – processes in which citizens are expected to actively participate.'[33] Both sides of republican freedom are put under pressure by modern data-driven applications, without necessarily infringing on the right to privacy of a particular citizen.

Citizens have little to no influence on the policy and affairs of big technology companies like Google, Apple and Facebook. Governmental organizations that are involved with the massive collection of data, such as intelligence services and special units of the police, are often subjected to limited democratic control (because transparency and democratic control would give the terrorists or criminal organizations knowledge about the operations of these types of governmental operations, which would undermine their effectiveness). In addition, these agencies build large databases and acquire knowledge and thus power over citizens and society as a whole, while legal safeguards against arbitrary power and judicial oversight are minimal (the procedural side of the use of arbitrary power) and data gathering programs, like mass surveillance, CCTV camera's and data retention of internet traffic, are often applied in a context-blind manner (the material side of arbitrary power). They affect potentially everyone, without taking into account the specific context in which they are applied or the background of the specific persons that are effected. The NSA simply collected all the information it could put its hands on, cameras film everyone and always when in their sight, Google collects data from almost everyone using the web, etc.

Because the liberal principle of 'non-interference' seems ill-suited for these types of modern data processing operations, more and more privacy scholars are proposing to embrace instead the republican model of freedom as non-domination, at least for these types of data-driven applications. For example, Andy Roberts made the following observation about the positive interpretation of freedom in republican theory: 'Privacy scholars have taken up this idea and suggested that we should think about the harm to which the loss of informational privacy gives rise in terms of the power that others acquire over us as a consequence. But those who have acknowledged the relationship between surveillance, loss of privacy and the

[31] <https://plato.stanford.edu/entries/republicanism/>.
[32] F. Lovett & P. Pettit, 'Neorepublicanism: A normative and institutional research Program', Annual Review of Political Science, 12, 2009.
[33] A. Roberts, 'A republican account of the value of privacy', European Journal of Political Theory 2015, Vol. 14(3), p. 337.

acquisition of power appear to have recognized neither the importance of participation in political decision making as means of controlling power nor the role of privacy in facilitating such participation.'[34] In similar vein, Bryce Newell suggests that the negative understanding of freedom in republicanism 'provides valuable insights into how one-sided surveillance powers and control of information vested in states can limit individual freedom. Applying neorepublican political theory in this context represents an important and novel application of these valuable ideas with the capacity to inform future information policy research and the development of better laws and policies related to surveillance, secrecy, and access to information.'[35]

5. The ECtHR as a republican court?

Interestingly, it is the European Court of Human Rights that seems susceptible to these kind of arguments. As described in section 2, in its dominant case law, the ECtHR is a clear and univocal proponent of the liberal theory, in which privacy is seen as freedom from interference. It requires that a claimant can demonstrate concrete and actual harm, following from a concrete and actual interference with his rights and freedoms. Applications about a law or a policy as such, which have not have a direct effect on the applicant, are declared inadmissible. Cases that regard societal interests, the interests of others or hypothetical harm are rejected by the Court, because it demands prove of an actual interference with the claimant's freedom. However, the European Court of Human Rights is increasingly faced with complex data driven cases in which concrete damage and individual harm are difficult to substantiate, while at the same time, there are clear and evident problems at stake. An example may be the trend that countries allocate large powers to the police and intelligence agencies to collect and use data, while at the same time laying down minimal procedural safeguards and limited parliamentary and judicial oversight. When faced with these types of cases, the Court is willing to let go of the 'non-interference' principle. Three points are of special importance in this respect.

First, it should be recalled that under the European Convention on Human Rights, there is the so called three step test. If it has been established that the right to privacy of an applicant has been interfered with by a state, the case will be declared admissible. The matter of there being an interference or not is only the first question. The second question is whether an interference was legitimate or not. If a restriction (1) is prescribed by law, (2) serves a legitimate aim and (3) is necessary in a democratic society, the interference will be deemed legitimate and there will be no violation of Article 8 ECHR. To determine whether an infringement was prescribed by law, the question is whether there was a legal basis granting a power to the governmental organization involved and whether the conditions for using that power were respected. For example, the police may be granted a power to enter the home of an individual, but only if it has a warrant from a court or prosecutor. If the police then enters the home of an individual without such a search warrant, one of the conditions for the use of power has not been met and the interference will not be deemed to have been prescribed by law. Linked to the criterion of a legal basis is the requirement that the law must be clear, must be made public and must be foreseeable as to its consequences. [36]

Over time, the European Court of Human Rights has introduced another sub-requirement under the criterion that an interference must have a legal basis, namely the 'quality of the law' requirement. Interesting is that the Court places particular emphasis on the

[34] Roberts, p. 336.
[35] B. C. Newell, 'Technopolicing, surveillance, and citizen oversight: A neorepublican theory of liberty and information control', Government Information Quarterly 3, 2014.
[36] <http://ysu.am/files/Davit_Melkonyan-1415702096-.pdf>.

safeguards against the arbitrary use of power when it analyses the quality of laws. Inter alia, it has ruled: 'Since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.'[37] Consequently, the Court places emphasis on the principles connected to the rule of law, on whether or not unfettered power is granted to government agencies and on the existence of safeguards against 'arbitrary interferences'. This 'quality of law' requirement implies that a law (1) must clearly describe what powers are assigned to the governmental agency, (2) the terms and conditions under which it can use these powers, (3) what parliamentary and judicial oversight is applied to the use of power and (4) what safeguards and remedies are in place for citizens.

These are all principles that are emphasized especially in republican theory. Still, it could be argued, the European Court of Human Rights still requires an actual 'interference'. As stressed above, the first question is whether an interference has taken place. If this has not been established, the Court will not come to answer the second question, namely whether the three-step test (including the requirement of 'quality of law') was correctly applied. As described in section 2, normally, the ECtHR requires an actual infringement and concrete harm and will thus reject so called *in abstracto* claims, which revolve around a law or policy as such. This would mean that governments involved in large-scale covert data collection programs would be relieved from the supervision of the European Court of Human Rights as it is. The Court, recognizing this problem, has recently explicitly acknowledged that in some cases, it needs to let go of the requirement of actual and concrete harm and of the liberal 'non-interference' principle.[38]

The first time it did so explicitly was in the case of Zakharov v. Russia, regarding mass surveillance powers attributed to the Russian intelligence agency. The case dates from December 2015.[39] The complaint regarded Order no. 70 of the Russian State Committee for Communications and Information Technologies, on the basis of which the mobile network operators had installed equipment which permitted the Federal Security Service (FSB) to intercept all telephone communications without prior judicial authorisation. The applicant argued that although Order no. 70 had never been published, he believed that his right to privacy under Article 8 of the European Convention on Human Rights had been violated. The government stressed that the applicant could not claim to be a victim of the alleged violation of his right to respect for his private life or correspondence, as he did not know whether he was affected or not and could not produce any evidence to substantiate his beliefs. Moreover, the applicant had not exhausted domestic remedies. The Court, however, ruled differently.

'[T]he Court accepts that an applicant can claim to be the victim of a violation occasioned by the mere existence of secret surveillance measures, or legislation permitting secret surveillance measures, if the following conditions are satisfied. Firstly, the Court will take into account the scope of the legislation permitting secret surveillance measures by examining whether the applicant can possibly be affected by it, either because he or she belongs to a group of persons targeted by the contested legislation or because the legislation directly affects all users of communication services by instituting a system where any person can have his or her communications intercepted. Secondly, the Court will take into account the availability of remedies at the national level and will adjust the degree of scrutiny

[37] ECtHR, Malone v. the United Kingdom, application no. 8691/79, 02 Augustus 1984.
[38] See also: ECtHR, Szabó and Vissy v. Hungary, application no. 37138/14, 12 January 2016.
[39] ECtHR, Roman Zakharov v. Russia, application no. 47143/06, 04 December 2015.

depending on the effectiveness of such remedies. [W]here the domestic system does not afford an effective remedy to the person who suspects that he or she was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such circumstances the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8. There is therefore a greater need for scrutiny by the Court and an exception to the rule, which denies individuals the right to challenge a law *in abstracto,* is justified.'[40]

It then went on to apply what could essentially be seen as an analysis of the quality of the law. It assessed, inter alia, the accessibility of domestic law, the scope of the application of secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation of secret surveillance measures, the supervision of the implementation of secret surveillance measures, the notification of secret surveillance measures, the available remedies and the duration of the secret surveillance measures. It found problematic aspects on all or most of these points and concluded 'that Russian legal provisions governing interceptions of communications do not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which is inherent in any system of secret surveillance, and which is particularly high in a system where the secret services and the police have direct access, by technical means, to all mobile telephone communications. In particular, the circumstances in which public authorities are empowered to resort to secret surveillance measures are not defined with sufficient clarity. Provisions on discontinuation of secret surveillance measures do not provide sufficient guarantees against arbitrary interference. The domestic law permits automatic storage of clearly irrelevant data and is not sufficiently clear as to the circumstances in which the intercept material will be stored and destroyed after the end of a trial. The authorisation procedures are not capable of ensuring that secret surveillance measures are ordered only when "necessary in a democratic society". The supervision of interceptions, as it is currently organised, does not comply with the requirements of independence, powers and competence which are sufficient to exercise an effective and continuous control, public scrutiny and effectiveness in practice. The effectiveness of the remedies is undermined by the absence of notification at any point of interceptions, or adequate access to documents relating to interceptions.'[41]

Consequently, in a small number of cases, which revolve mainly around secret mass surveillance programs by intelligence agencies, the European Court of Human Rights will accept so called *in abstracto* claims. Doing away with the victim requirement and the principle of 'non-interference' means that a number of other criteria connected to these principles are also redundant in these types of cases, such as that legal persons cannot complain about a violation of the right to privacy, that cases revolving around societal interests are not declared admissible and that cases that revolve around minimal harm only (the *de minimis* rule)[42] are not taken into account by the Court. What it will do in these types of cases is mainly assess the 'quality of law' requirement. Is the law made public, is the law understandable, does the law set limits to and conditions for the use of power, are there sufficient means of oversight, are there checks and balances against the arbitrary use of

[40] Zakharov, § 171.
[41] Zakharov, § 302.
[42] Article 35 (3) (b) European Convention on Human Rights.

power, are there remedies for citizens, etc.[43] This leads to the third and final point, namely that the European Court of Human Rights is increasingly adopting a role as a European constitutional court, rather than as a classic human rights court. In countries such as Germany and France, the supreme court is already authorized to test parliamentary laws and governmental policies on the various aspects of the rule of law, even when there is no individual complaint and the freedom of citizens has not been interfered with. It is an abstract test. This review of 'constitutionality' is in many respects the same as the test that the ECtHR applies in *in abstracto* cases, namely assessing whether the law or policy as such provides sufficient safeguards and adheres to the principles connected to the rule of law. [44]

Not surprisingly, the European Court of Human Rights increasingly uses a term that is derived from the word 'constitutionality', namely the 'conventionality' of national laws and policies.[45] 'The abstract review of "conventionality" is the review of the compatibility of a national law with the Convention independently of a specific case where this law has been applied.'[46] It is important to recall that cases are normally only declared admissible under the European Convention on Human Rights if all national remedies have first been exhausted (the complainant has brought the matter to the national court, filed appeal and then submitted his case to the national Supreme Court).[47] Even when all domestic remedies have been exhausted, the European Court of Human Rights will not act as a court of fourth instance.[48] This means that it will normally not reconsider the case in full, but will only assess whether a human right has been trampled. It is interesting to see that even this principle is abandoned when the ECtHR acts as a European constitutional court – in such matters, it is even prepared to act as a court of first instance. 'In other words, the Grand Chamber invests itself with the power to examine *in abstracto* the Convention compliance of laws without any prior national judicial review.'[49]

6. Conclusion

Section 2 showed that the right to privacy is currently primarily linked to the individual, his rights and his interests. An application under the European Convention on Human Rights is declared admissible only if the complainant can demonstrate that there has been a specific interference with his right to privacy, resulting in actual harm. Section 3 described that with respect to modern data technologies, it is increasingly difficult to identify concrete infringements and to substantiate personal harm that has resulted therefrom. Section 4 indicated that a number of privacy scholars has argued that another approach to privacy should be adopted with respect to these types of cases; primary attention should not be paid to the liberal 'non-interference' principle, but to the republican 'non-domination' principle, which lies emphasis on power relations as such and the potential for arbitrary use of power.

---

[43] B. van der Sloot, 'Is the Human Rights Framework Still Fit for the Big Data Era? A Discussion of the ECtHR's Case Law on Privacy Violations Arising from Surveillance Activities', In: S. Gutwirth, R. Leenes & P. De Hert (eds.), 'Data Protection on the Move', Springer, Dordrecht, 2016, pp 411-436.

[44] ECtHR, Michaud v. France, application no. 12323/11, 06 December 2012. See also: ECtHR, Vassis and others v. France, application no. 62736/09, 27 June 2013.

[45] See for the use of the word also: ECtHR, Py v. France, application no. 66289/01, 11 January 2005. ECtHR, Kart v. Turkey, application no. 8917/05, 08 July 2008. ECtHR, Duda v. France, application no. 37387/05, 17 March 2009. ECtHR, Kanagaratnam and others v. Belgium, application no. 15297/09, 13 December 2011. ECtHR, M.N. and F.Z. v. France and Greece, application nos. 59677/09 and 1453/10, 08 January 2013.

[46] ECtHR, Vallianatos and others v. Greece, application nos. 29381/09 and 32684, 07 November 2013, partly concurring, partly dissenting opinion of judge Pinto de Albuquerque.

[47] Article 35 (1) European Convention on Human Rights.

[48] <http://www.echr.coe.int/Documents/Rules_Court_ENG.pdf>.

[49] ECtHR, Vallianatos and others v. Greece, partly concurring, partly dissenting opinion of judge Pinto de Albuquerque.

Section 5 indicated that the European Court of Human Rights already seems to embrace the republican approach to privacy in a small number of cases. It is willing to assess *in abstracto* claims and assess the quality of laws and policies acting as a European constitutional court, inter alia, when cases regard covert mass surveillance activities by intelligence agencies. No concrete interference or personal harm is required.

What the precise consequences of such a shift may be is unclear, but three potential developments could emerge. First, there are signs that the republican approach to human rights violations will not be limited to cases in which data-driven applications are at stake.[50] This could mean that in time, the European Court of Human Rights would expand its role as a European constitutional court and will assess all or most national laws that have an impact on the provisions under the European Convention on Human Rights on aspects connected to the rule of law. If this trend indeed emerges, it may receive cases as a court of first instance and analyze whether the laws and policies respect the basic principles aligned to the notion of 'quality of law'. Are the laws clear and accessible, do they describe clearly what types of power are assigned to governmental agencies and under which conditions they may be used, are there remedies in place for citizens and is there adequate parliamentary and judicial oversight? These are the types of questions that the ECtHR could answer with respect to all matters brought to its attention with respect to the right to privacy and potentially other doctrines; from a republican perspective, there is no limit to applying these types of questions – all competences granted to governmental organizations are relevant as they can always have a potential impact on the power relationship between the citizen and the state.

The second development on which this new approach of the European Court of Human Rights may have an impact is the debate about whether the regulation of information should be limited to 'personal data' or whether it should be extended to all 'data'. The current regime, for example under Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[51] of the Council of Europe and the European Union's General Data Protection Regulation[52] and the Police Directive,[53] use the concept of 'personal data'. On the one hand, there are arguments to extent this scope to all 'data', because data in general can be used to influence people and to make decisions that have a high impact on society as a whole and the groups living therein. On the other hand, the question is often posed, 'what is the problem of gathering data?', or put differently, 'what harm does it do when non-personal data is gathered?'. These are difficult questions to answer using the liberal 'non-interference' principle. But reasoning from a republican ideal of freedom as non-domination, the fact that with data gathering and possession comes power is enough to regulate these data flows.

The third and final development on which the republican approach of the European Court of Human Rights may have an impact is on the regulation of the analysis of data. The current data protection instruments focus primarily, though not exclusively, on the gathering

---

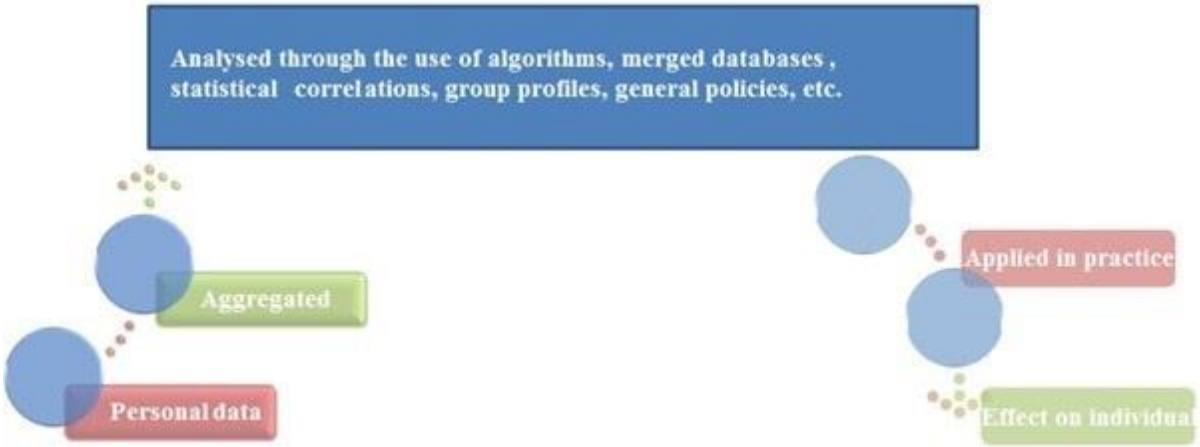
[50] For the use of the term 'conventionality', see among others: ECtHR, Kennedy v. the United Kingdom, application no. 26839/05, 18 May 2010. ECtHR, Suso Musa v. Malta, application no. 42337/12, 23 July 2013. ECtHR, Orchowski v. Poland, application no. 17885/04, 22 October 2009. ECtHR, S.A.S. c. France, application no. 43835/11, 01 July 2014. ECtHR, Duong v. Czech Republic, application no. 21381/11, 14 January 2016. ECtHR, Maslak and Michalkova v. Czech Republic, application no. 52028/13, 14 January 2016.

[51] <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37>.

[52] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[53] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

and the storage of data. Other instruments regulate the use of data, for example when it has a discriminatory impact on groups with a certain ethnic, religious or cultural background.[54] The reason to regulate the access to and the use of data is that at these moments, the individual and his interests are still in sight. The phase in between, however, in which the data is analyzed, is currently mostly left unregulated. Here, however, the real decisions are made in terms of how data are combined, which terms are used to analyze them, which algorithm is applied, how different databases are merged, which statistical correlations are selected as significant, how group profiles are built and which general policies are derived from the correlations. All these choices have no direct and concrete impact on individuals, so that it becomes hard to regulate this phase using the liberal idea of freedom of non-interference. When the principle of non-domination is accepted, however, it is enough that these choices, the group profiles developed and the policies based thereon are means to secure and use power, and therefore should be subject to regulation and control.



[54] See of course also: Article 14 of the European Convention on Human Rights.