COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle

Bart van der Sloot *

Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, Netherlands

Keywords:
Republicanism
Non-interference
Non-domination
Big data
Privacy

A B S T R A C T

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 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 advocate 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 domains, both spheres are becoming increasingly blurry. Smart devices are entering the home and along with them is 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

* Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, PO Box 90153, 5000 LE Tilburg, Netherlands.
E-mail address: b.vdrsloot@uvt.nl.

https://doi.org/10.1016/j.clsr.2017.11.013

[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).

Please cite this article in press as: Bart van der Sloot, A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.013

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

These are more specific challenges for the current approach to the right to privacy catalysed by technological and societal developments. But there is also a more fundamental question that is becoming ever more urgent. Both in literature and in the legal discourse, privacy is regarded as a subjective right of the natural person to protect his/her personal interests, such as relating to human dignity,[6] individual autonomy[7] and personal freedom.[8] To determine whether the right to privacy has been violated, the principle question that is asked is whether there has been an 'interference' with this right. In reality, however, it is increasingly difficult for individuals to specify how and to what extent they are individually harmed by Big Data and mass surveillance practices, as the individual element is increasingly difficult to substantiate. Interestingly, both in literature and in legal practice, an alternative approach has been suggested, in which the core question is not whether there has been an 'interference' with a right, but whether there is a power relation in which there exists 'domination'. This article discusses this trend by analysing, by way of example, the jurisprudence of the European Court of Human Rights (ECtHR) and by interpreting case law from a philosophical perspective.

Section 2 explains that the privacy case law of the European Court of Human Rights is predominantly focused on the question of whether there has been an 'inference'. Section 3 discusses how new data-driven applications challenge this approach, inter alia because it is increasingly difficult for claimants to demonstrate a concrete 'infringement' and to specify harm. Section 4 shows that in recent years, the ECtHR is prepared to let go of its focus on actual infringements and concrete harm in cases revolving around, inter alia, mass surveillance. Section 5 argues that this shift may be understood from a more theoretical perspective as a move away from a tradition to which 'interference' and harm are central concepts, and towards a republican approach, in which 'domination' and arbitrary forms of power are central elements. Section 6 concludes by showing that besides the ECtHR, the European Court of Justice is also willing to accept a focus on 'domination' rather than 'interference' in a number of cases, and points to some potential effects this new approach by the European courts may have on the future of privacy regulation.

2. How the ECtHR usually approaches privacy cases

Article 8 of the European Convention on Human Rights (ECHR) provides: '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.'[9] 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.'[10] 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.'[11] 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

[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.

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

[10] Article 33 of the European Convention on Human Rights.

[11] Article 34 of the European Convention on Human Rights.

Please cite this article in press as: Bart van der Sloot, A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.11.013