Privacy Limitation Clauses: Trojan Horses under the Disguise of Democracy

van den Hoven van Genderen, R.

2016

document version
Publisher's PDF, also known as Version of record

Summary

The essence of this thesis is the dynamic character of privacy as dependent on place, time, culture and political climate and the need to mold this right to the needs of the common good of society. This process is a never-ending story already known in the Greek city states and probably even before that time.
Privacy, the protection of the personal sphere and personal data in particular, by non-intervention by the government, is a fundamental right for citizens but not an absolute right.
Historically the citizens of a society decided theoretically to transfer a part of their individual rights to an authority for the general interest of society.
Although many legal philosophers such as Hobbes, Locke, Rousseau, and even a prominent privacy thinker, Westin, all accept that the exercise of rights of citizens can be transferred in the public interest, there should always be a personal right to (informational) self-determination. Some states, such as the German Federal Republic, are very clear about this by stating this right as such in their constitution. But even Germany accepts that there are circumstances that intrusion into the right to privacy is necessary to secure their democratic society.

This means that the government may curtail this right if the circumstances so require. This is notably the case when there is a threat to national security or any other threat to our democratic society. These limitation possibilities are enshrined in international treaties like the Universal Declaration of Human Rights, the ICCPR and in particular the second part (paragraph 2) of Article 8 of the European Convention for Human Rights (ECHR). The limitation grounds and policies based upon these limitations are integrated in the Member States' legislation. These limitations and considerations are also reflected in EU law and in the legal systems of several non-European countries such as the US by using the possibilities given in the Patriot Act and comparable legislation. The restrictions are not only found in the legislation on the investigative powers of security and justice, but also in telecommunications law and economic and financial (money laundering) legislation.

My research question was whether it is possible to create such restrictions on the right to privacy in such a way that they remain compatible with principles of a democratic society a democratic order

Because of the vulnerability of the privacy of citizens, restrictions are to be reigned by a set of objective requirements: they must comply with the law; be necessary for the democratic rule of law; be proportional as to the result to be achieved; and, they must be enacted in accordance with accessible and foreseeable legislative transparency of the rules. It is important that law that limits privacy does not contain or consists of vague concepts and definitions or unclear competences for legal enforcement agencies and other governmental agencies. The main obstacles, as described in this thesis, to finding a justified result in the balancing between the individual and general right to privacy., and the acceptable intrusion by authorities, are due to the peculiar vagueness of definitions and the dis-harmonisation of regulations amongst the states that have to apply those regulations. This thesis analyses in this context law on anti-terrorism, anti- money laundering, mainly to support terrorist activities and data retention rules.

In several rulings of the European Court of Human Rights and the European Court of Justice deal with the (un) lawfulness of the restrictions. The most revolutionary ECJ case in this respect was the annulment of the so called retention directive on April 8 2014, because the legal justification to store telecommunication data of all European citizens lacked legitimation and legal guarantees.
The other legal peculiarity that is described in this thesis is the fact that soft law, without too much hesitation, is transferred into hard law. This is for instance the case in the field of anti-money laundering and terrorist financing by the so called' Financial Task Force, FATF that creates a soft-law framework. These 'informal' deliberations to prevent money laundering and terrorist financing have led to a list of 49 principles which are almost literarily copied into EU legislation as the 4th Anti-Money Laundering Directive and national law implementing this Directive.
The result is that rather vague concepts as the 'risk based' principle are accepted in international and national law for the investigation and prosecution of money-laundering and anti-terrorism without proper definition or even a description of its meaning.
These concepts are the result of the fact that advanced technological developments result in more intrusive techniques, available for governmental agencies in enforcement as well available to terrorists and other criminals. The activities of the aforementioned parties are used by legal enforcement agencies to justify the use of further intrusive techniques and policies to perform their tasks to prevent the risk of undermining our democratic societies.

.
What I have found in my research is that privacy and protection of personal data are subject to the dynamics of the political situation, as well as the availability of new intrusive technologies. It shows a wave cycle: After a wave of new rules to increase the competencies for intelligence and law enforcement after 9/11, we see a softening and critical notion on those activities after the revelations of Snowden and the disclosures of intelligence agencies spying on each other and on their own and foreign citizens and politicians with the help of information-technology. Lately, there is again a reinforcement of surveillance and interception powers after the terrorist attacks in Paris and Brussels. Surveillance acts in the UK, France and the Netherlands are criticized but have passed through parliament without too much trouble. The citizens themselves should be more involved in the size of the transfer of their privacy rights and whether the government is intruding on their privacy in a proper and justified way. This should be done by a more active and controlling role of the parliament and an independent control authority with regard to the implementation of the mitigation measures.
This conclusion regarding independence and clarity of scope of responsibilities and definitions, is drawn by both the European Court of Justice regarding the unlimited storage and use of telecommunications data of citizens, as well as by the European Court of Human Rights in respect of the use of advanced interception and surveillance techniques.
There should be no choice between the justification of the right to protection of national security against terrorism on the one hand and privacy on the other hand. The government has a duty and responsibility to ensure both "rights" through the implementation of rules and policies. If a government does not abide by this principle, or is willfully acting contrary to the demands of a democratic order by restricting fundamental rights, there is no legitimization of its existence. In an important ruling of the ECtHR, the Court states that the restrictive measure on a fundamental right to secure democratic society may never have the impact that the fundamental right

disappears and consequently the democratic system that is based on those fundamental rights. It is therefore of utmost importance that an independent balancing of interests mechanism consists in the introduction and implementation of privacy restrictions which is taking into account all the interests of a democratic order.

As concluded in this thesis the leading principle in this balancing process should be the proportionality test. According to the settled case-law of the ECtHR and the ECJ, an act of a state authority as well as the European Union may be regarded as proportionate when the measures which it implements are appropriate for attaining the objectives pursued and do not go beyond what is necessary to achieve those objectives. Additionally,the so called Siracusa Principles that I discuss in this thesis, provide a more transparent balancing process. Looking out to a 'geo-logical' landscape of increasing information, communication and robotic technology, and the perceived existence of uncontrollable terrorist threats, creates the attraction for law enforcement and intelligence agencies to use these techniques on a wide scale to pursue 'persons of interest'.
When limitations on privacy are not defined specifically in law and the use of intrusive competencies and techniques are not strictly demarcated, the proportionality principle and the balancing process will be hollow instruments. There always will be an uncontrollable competence of policy concerning national security and other strategic interests of the state within the institutional framework. This aspect is even strengthened by the existing dichotomy between the interests of authorities in their role of privacy regulators and legal enforcement agencies.

The difficult tasks of governments in this vulnerable information age is to find a credible solution to balance the individual privacy as well as the common principle to protect such fundamental rights to deserve the notion of democratic society with other common principles such as creating a safe society for citizens.

If there is an acceptable solution, it has to be found in a dynamic system of privacy controls that will keep pace with changes in society and technological developments with a keen eye on the fundamental integrity of the personal life of citizens all over the world.