COMPUTER LAW & SECURITY REVIEW 34 (2018) 920–923

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

Digital justice

Corien Prins[a,b,*]

[a] Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands
[b] The Netherlands Scientific Council for Government Policy (WRR), the Netherlands

ARTICLE INFO

Article history:

Keywords:
Constitutional power
State powers
Checks and balance
Judiciary
Legal analytics

ABSTRACT

In a period of growing suspicion about the power of digital technology and 'tech companies', this short comment aspires to argue that the conditions for the functioning of the constitutional state contain an inherent obligation for the state not only to be sufficiently sensitive to the changes brought about by digitisation, but also to make use of digitisation. A key condition for the functioning of the constitutional state is e.g. that the judiciary is capable of fully implementing its task of affording legal protection. Reinterpreting this condition in the modern age implies that courts should remain explicitly vigilant when it comes to digitisation. Hence, affording protection is not only a question of what makes formal regulation in a digital world different from regulation in the well-known offline world. If the constitutional state is to be 'capable' of implementing its task of affording legal protection, it must also be sufficiently sensitive to the changes brought about by digitisation, as well as deploy the potential that digitisation offers.

© 2018 Corien Prins. Published by Elsevier Ltd. All rights reserved.

1. Regulative capacity and constitutional power in the digital world

An immensely rich and broad spectrum of articles and other contributions published in the previous 199 issues of this journal, have pointed out the disruptive impact and turbulent nature of so many developments that resulted from the introduction of ICT and thus the digitisation of our society. The many insights presented have shown, among others that the process of legal development – and of formal legislation especially – struggled with the high propagation speed of new technologies and the resulting social as well as legal problems. In addition, digital technologies and its applications erode to a large extent the power of national government authorities to act. Aside from the cross-border implications of digital innovation, it makes citizens less dependent on – and more autonomous with regard to – existing hierarchies, such as the national government. In addition, power that used to be exerted by the government is now sometimes in the hands of tech giants such as Facebook, Google and Uber. The 2018 Cambridge Analytica scandal brought into sharp relief how these entities are capable of abusing their power on a worldwide scale. In sum, the digitisation and abundant data flows has led to fundamental and irreversible social developments that require the role of the government in all its tiers to be reconsidered. For if the developments are ignored, politics and policy may lose their regulative capacity in the field of digitisation.

No surprise then, it is argued that government requires greater vigilance regarding many crucial questions raised by these developments. Regulatory interventions need to be considered, given the state's responsibility to equip citizens with the tools for carrying out their own control. However, although European and other legislators still seem to assume that citizens should be able to exert 'control' in the digital world, the reality of our modern data-driven society shows that individuals are often unaware of what data are processed about

* Corresponding author: Institute for Law, Technology, and Society (TILT), Tilburg University, P.O. Box 90153, 5000 LE Tilburg, the Netherlands.
E-mail address: J.E.J.Prins@uvt.nl

https://doi.org/10.1016/j.clsr.2018.05.024
0267-3649/© 2018 Corien Prins. Published by Elsevier Ltd. All rights reserved.

them, how they are judged and categorised by businesses and the government, and what the consequences are for them. Would this mean that the state has a bigger role to play in the information society? Irrespective of the answer to this question, it becomes a challenge to envision which actors and institutions should participate in the process of enforcing the position of citizens and making the public aware of what is happening in our present-day society. Some actors might be effective (hacktivists) but they seem to lack legitimacy in what they do. Others might be considered to have legitimacy (sovereign states), but sometimes lack the necessary digital awareness, actual power and influence in the online world. At the same time, as we all know, it is both undesirable and unnecessary to strive for a controlling role in the information society. It is not the government's responsibility to manage all risks. Having said that, administrative and legal institutions have constantly to explore their role and responsibility in dealing with the changes, for there are tremendous risks if both the law and public administration are so to speak "swept along" by technology-based changes and end up in a permanent state of flux.

In the light of this, my argument here is that fortifying the very conditions for the effective functioning of the law, implies that all constitutional powers of the state exercise an inherent obligation to understand and make use of digitisation. Let me illustrate my point with the constitutional value of proper law enforcement. Such enforcement – in the criminal, civil and public administration spheres – is one of the most important conditions for maintaining the ethos of the constitutional state. For example, insufficient investigative capacity among the police and judiciary can, in the long term, serve to undermine confidence in the rule of law. In essence, the same applies to the digital sphere. Effective enforcement of administrative law (e.g. privacy and competition regulations) by supervisory institutions (e.g. data protection authorities) and the courts, is just as essential to the constitutional state in the digital domain as the enforcement of these regulations is in the offline world. A lack of government response to breaches of the law in the digital domain can also serve to undermine citizens' confidence in the rule of law. As a result, it is essential for the government to enforce the law in both the analogue and digital worlds.

Here, digital resources can be of great assistance in both the online and the analogue world. Neighbourhood Apps are much quicker at letting the police know what is happening at the local level. Videos taken by local residents with their mobile phones can serve as evidence in potential court cases. 'Big data' sometimes allow tax authorities to 'predict' tax evasion, i.e. to know the likelihood of certain people breaking the law under certain conditions and during certain periods. And indeed, during the past decade, many public bodies (police, security agencies, tax authorities, organisations in youth care and other public policy implementing bodies) have embraced digitisation. More recently, these and other organisations have started implementing practices in which the use of what is now commonly referred to as big data, i.e., the smart deployment of data analysis techniques, is a key factor in implementing policy and legislation. Illustrative are domains such as safety and security, traffic management and environmental protection. Data analytics allows such implementing bodies to gain a better understanding of e.g. child abuse, reasons for migration, or patterns related to subversive crime. Clearly, investigate and executive authorities can profit significantly from big data in combining hindsight (pattern analytics), insight (real-time analytics) and foresight (predictive analytics).

2. Checks and balances

However, implementing the promises of digital innovation should not be restricted to these powers of the state. A key condition for the effective functioning of the constitutional state is that the courts be capable of fully implementing its task of affording legal protection. Reinterpreting this condition in the modern age implies that courts should remain explicitly vigilant when it comes to digitisation. Hence, one of the challenges for courts is the need to address the question of what makes legal protection in a digital world different from legal protection in the well-known offline world. If the judiciary is to be 'capable' of implementing its task of affording legal protection, it must also be sufficiently sensitive to the changes brought about by digitisation. Put simply, to use a term applicable to the younger generation that has grown up in a digital world, it must be 'tech savvy'. In constitutional terms, under the broader constitutional assurance of checks and balances, it is not only the executive and legislative powers but also the courts that must be capable of performing such checks and balances.

An illustrative example of the importance of checks and balances is when, as discussed above, executive authorities start using pre-installed algorithms. As discussed and analysed in many contributions to this journal authorities, such as tax authorities or social insurance agencies, make automated decisions on income or allowances, often based on such algorithms. Such systems are efficient and practical when they work, i.e. if the decision-tree used by the algorithm is a correct interpretation of the underlying legislation. When formulating algorithms, however, statutory provisions either can prove to be too vague or may be interpreted too generally. The digital system is unaware of the power that public officers have to grant exceptions. The decisions, which it makes, are 'digital' (black-and-white) and the default is that the algorithm is correct. If citizens do not agree with the decision, their only available option is to lodge an objection or go to the administrative tribunal. This then implies that supervisory bodies and courts are capable of assessing algorithmic-based decisions. In many instances, however, due to a lack of information on the specifics of how the algorithm is structured or results produced, such an assessment is highly problematic. However, demanding accountability from administrative bodies is crucial and courts must oblige them to make all algorithms public and accessible (in a manner comprehensible to the average citizen). For only when the data, algorithms and assumptions on which they are based are made public (in good time and on their own initiative), can the checks and balances of our constitutional state properly function?

Checks and balances in a digital world ultimately mean that state authorities must be able to engage in a digital sense, rather than leave the responsibility for justification and accountability with other. In other words, the functioning of the

Download English Version:

https://daneshyari.com/en/article/6890444

Download Persian Version:

https://daneshyari.com/article/6890444

Daneshyari.com