

Social and Ethical Shifts in the Digital Age: Digital Technologies for Governing or Digital Technologies that Govern?



Paolo Depaoli, Maddalena Sorrentino, and Marco De Marco

Abstract Organizational efficiency and economic development has benefited significantly from the ubiquitous nature of information technology in today's governmental machinery and in society, but what of its serious implications at the macro and micro level? The argument of the paper is that technology-driven social changes require—and facilitate—a policy response. Exploring the wider implications of ICT used by governments through the lenses of two analytical frameworks (i.e., the 'tools of government approach' and the 'data-driven agency approach') elaborated in two seminal books allows us to formulate a number of information policy recommendations for contemporary decision makers seeking viable solutions to ethical concerns. The conceptual discussion aims to spur an early and pro-active engagement with the social impacts of technology.

Keywords E-government · Tools of government · Data-driven agency · ICT policy · Ethics · Social impacts of ICT

1 Introduction and Impetus of the Study

Handling the impacts and consequences of technology has become a problem of political, social and academic relevance since the Sixties [1]. Today, unlike the pre-digital era, the intertwining of 'society' and 'technology' [2] has acquired even greater importance and has no equivalence in terms of scale, scope, integration and

P. Depaoli (✉)
Sapienza University of Rome, Rome, Italy
e-mail: paolo.depaoli@uniroma1.it

M. Sorrentino
University of Milan, Milan, Italy
e-mail: maddalena.sorrentino@unimi.it

M. De Marco
International Telematic University Uninettuno, Rome, Italy
e-mail: marco.demarco@uninettunouniversity.net

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2021

C. Metallo et al. (eds.), *Digital Transformation and Human Behavior*,
Lecture Notes in Information Systems and Organisation 37,
https://doi.org/10.1007/978-3-030-47539-0_21

capability [3]. Many commentators are by now convinced that current developments may change the very fabric of society in a short period of time [4, 5].

A global issue with a far-reaching impact on public expectations is e-government. Many years have passed since the use of digital ICTs for the conduct of government stopped being a stand-alone issue to become a cross-cutting issue. At the ‘government-society interface’ level [6:17], the transformational impact of ICTs is manifested mainly in the way governments use digital technologies to gather information and influence individual and firm behaviour. But there is more at play. ICTs also involve a change in values or in the value system: according to Bannister and Connolly [3:119], almost any ICT implementation in the public sector will have implications for public values. Further, governmental technology policy creates obligations for everyone [7:21].

Hence, the transformative potential of ICT has truly become a game changer of the social context. Notable examples of new generations of ICT that enter the public arena bring with them unprecedented, ethically relevant questions and implications regarding, for example, analytics, artificial intelligence and virtual/augmented reality. And, while the main talking points of public opinion centre on key issues such as privacy and surveillance, the debate fails to address other, just as relevant cross-cutting issues. To date, far less envisaged and explored are the critical questions: How legitimate is the techno-regulation exercised by the private digital giants? Are the consumers truly aware of the rules embedded in the ICT artefacts or in the online services they use in the everyday lives?

Against this background, it is essential to understand what is happening and with which consequences. The OECD [8] very recently published a document stating that the role of public services is being questioned due to the effect of the increasingly pervasive presence of the global digital players in areas such as broadcasting, postal services, libraries and social meeting spaces. The OECD goes on to say that where the rationale for public intervention may have eroded, the governments and regulators need to apply a ‘rethinking’ [8:28].

Getting a clear and unobstructed view of the underlying nature of the changes spurred by digital transformation is prerequisite to ensure policy responses better tailored to the times we live in. Despite the crucial issues raised by privacy threats, public decision makers seeking to proactively address normative issues must push past the emotive response to news stories (such as the outrage sparked by the Cambridge Analytica scandal) to focus on what really lies beyond the immediate horizon.

The main purpose of this paper is to inform and increase awareness of the complexities of “moral and ethical concerns arising due of the social use of technologies” [9:21], and to sketch a range of recommendations for information policies. The need for brevity means that the approach taken here covers solely a handful of selected issues, building upon seminal studies that have addressed social and ethical shifts associated with the digital age from a variety of perspectives. Our interest is not the technologies *per se* but the generic interaction of ICT with society.

The article is organized as follows. After illustrating the research approach, the paper explicates the ‘instrumental’ and ‘relational’ perspectives of digital technology,

followed by a nuanced analysis of the ICT tools available to government in their broader context. The next section hosts the discussion and summarises the policy implications. The paper closes with the authors' final remarks.

2 Research Approach

The paper draws on two ground-breaking studies that have problematized the role of technologies in the public sphere, namely, the book by C. Hood and H. Margetts, *The tools of government in the digital age* (2007) [6], and that by M. Hildebrandt, *Smart technologies and the end(s) of law* (2015) [10]. The interest in these contributions is twofold, and lies precisely in the diversity (and, at the same time, the contiguity) of the analytical frameworks that inform them (policy studies and the theory of cybernetics, respectively, and legal and ethical studies). The books were written at two distinct periods in the timeline of the development and public visibility of the digital technologies. The 2015 essay shows a far more complex networked ty landscape than that considered by Hood and Margetts just eight years earlier.

The exploration follows two parallel tracks with the aim of highlighting for each of the two essays the way the ICTs are designed and the ethical consequences for the action of governments and for the information policies. The guiding question can be summarised as follows: *In what way do the different ways of conceptualizing the intertwining of society and technology contribute to the practice of government in the digital age?*

3 Digital Technology: 'Instrumental' or 'Relational'?

Much has been written and debated on the social implications of digital technologies [11]. Here, we start to map the methods with which the two essays in question, *The tools of government in the digital age* (2007) [6] and *Smart technologies and the end(s) of law* (2015) [10], have addressed the theme.

3.1 Digital Technologies as Tools of Tools

To understand the viewpoint of Christopher Hood and Hellen Margetts ("H&M"), it is necessary to know that the 2005 book was developed from Hood's earlier publication, *The tools of government* [12], written in the pre-digital age. The focus of the H&M essay is the interaction of the state with the citizens and the organisations through two macro categories of exchange-action instruments: (1) the 'detectors' or the information flows from individuals/organisations to the government ("all the instruments government uses for taking in information", p. 3), and (2) the 'effectors',

which are the influence flows that go in the opposite direction to the detectors (i.e. “all the tools government can use to try to make an impact on the world outside”, *ibid.*).

The two macro categories use four basic types of tools of government policy. *Nodality* denotes “the property of being in the middle of a social network”. *Authority* relates to “the ability to command and prohibit, commend and permit, through recognized procedures and identifying symbols”. *Treasure* indicates “whatever positive incentives or inducements government can use to secure information or change behavior”. Finally, *Organisation* denotes the possession of “stock of land, buildings and equipment, and a collection of individuals with whatever skills and contacts they may have”, somehow arranged. The authors say that any public policy will involve some mixture of these four basic resources.

The basic question continually evoked, even before indicating the effects of the digital technologies on the nodality, authority, treasure and organisation (“NATO”) instruments, is the way in which the authors consider such technologies. On the one side, H&M observe that, since the 1990s, Internet and the associated technologies have changed both the way in which many individuals behave in different social spheres and the way in which the governments interact with citizens and business. On the other, they argue that in many cases these (apparently) new instruments “can be understood as old instruments in a new technological context” (p. 14).

This position is resumed in the closing chapter of the book, in which the authors specifically reiterate the term ‘digital age’, confirming the instrumental role of digital technology: “we discuss the potential that the digital age may offer for a ‘sharpening’ of government tools, both to economize on governmental effort and to make government’s interactions with individuals less obtrusive (p. 185).” Further, the instrumental role of the technologies (which allows this ‘sharpening’) seems not to be affected by the organisational solutions adopted. In fact, the authors state in the introduction that their work “pays little or no attention to what goes on inside government’s organizational machinery” (p. xiii). Instead of considering the power games or the ‘convoluted decision processes’, their attention “focuses on the point where government meets individuals” (*ibid.*). Therefore, it would appear that the problem of the means-ends relationship can be solved only once the characteristics of the exchange instruments (opportunely updated to the state of the art of the digital technologies) have been defined, which happens at a certain point of interaction. In other words, it is a question of choosing the means best suited to the pursuit of a specific end.

To make this hypothesis hold water, we must assume that the technology plays a neutral role in social relations and, above all, in the organisations, and between these and the individuals that either belong to or have relations with it. In this respect, the authors state that:

Digital technologies have been hyped by some as fundamentally reshaping all human relationships, dismissed and ignored by others as irrelevant to the fundamentals of law and government. To get any grip on that slippery but important question, we need a method of analysis that is *technology-free*. (p. xiv our emphasis).

In a nutshell, the authors claim that a technology-free approach allows us to skip over complex and never-ending diatribes on the nature of the digital technologies (on this point, see [13]). Further, given that it is also organisation-free, the H&M approach enables us to move with agility among the substantially unchanged instruments (i.e., the government tools) and the ‘tools of tools’ (the digital technologies) that ‘sharpen’ the former. A further advantage in adopting a similarly technology-neutral framework is that it would allow us to understand what changes occur in the government toolkit when technology changes (p. 183). This latter observation by the authors does not seem to stray too far from technological determinism.

3.2 *Digital Infrastructures and Data-Driven Agency*

The pace of technological developments, in particular the Information and Communication Infrastructures (ICI), accelerated significantly in the eight years between the publication of H&M’s study in 2007 and Mireille Hildebrandt’s (“MH”) in 2015, when, taking a net position on the issue considered ‘slippery’ by H&M in 2007 (see above citation), the latter opined that: “Big Data is not a hype. It is here to stay. It is, however, a threat” (p. 226).

Hildebrandt maintains that the intertwining of relations between the diverse categories of actors and agents that use the new digital technologies whilst unknowingly being used is problematic. Although MH’s research was conducted in fields not strictly connected to the public sector, it is just as relevant because it concerns the consequences of the development of the ICTs that have caused the human agency to be affected by the ‘data-driven agency’.

Also for the purposes of this paper, the effects of such a development serve to understand how the ICIs are capable of conditioning not only the nature of the information exchange interface (detector), but also the influence (effector) of the four tools considered by Hood and Margetts. As a result, Hildebrandt argues that the digital technologies cannot be conceived as neutral tools.

MH suggests surpassing the instrumentalist and neutralist conception that disregards the values incorporated in technological devices to favour the view that sees technology—like the law—as a means of regulating the interactions between individuals and organisations and the behaviours of the various actors.

According to MH, conceiving technology in merely instrumental terms is problematic because it does not allow us to easily understand how a certain technology enables or impedes certain behaviours. Just as problematic is the explanation of how the interaction between individuals and environment changes when the technology used changes (p. 162). Rather, MH maintains that the technology itself already contains a normative and relational component and that the attention on and the research into the impacts of a technology must extend to the affordances, i.e., the potential of the tools or the artefacts, concluding that the assessment of technology cannot be limited to its intended usage or foreseeable functionalities (p. 172).

This aspect is particularly valuable in the case of the ICIs because many of the affordances that characterise them are *hidden* and concern ‘pre-emptive computing’, i.e., a computing based on predictive analytics combined with computational interventions that shape the human action, orienting it, supporting it or forcing it, before the human being can arrive at a conscious decision (p. 263). Here, Hildebrandt is referring to the configuration of a *digital unconscious*, i.e., a complex interweave of hidden inferences that increasingly reconfigure our digital environment (p. xiii), which, among other things, is increasingly integrated with the non-digital environment through the ubiquity of interconnectedness (p. 110).

The digital unconscious proposes real-time solutions-actions based on the preferences expressed unknowingly by the individuals during their online interactions and harvested, for example, through the practices of web profiling. Hence, MH maintains that we are witnessing a reduction of personal autonomy and, therefore, a growing difficulty in identifying responsibility at the individual level.

4 Digital Technologies for Governing or Digital Technologies that Govern?

These two different ways of thinking generate two different conceptions of the technologies used in the public sphere, prompting a much closer look.

4.1 *NATO Tools and Digital Technologies for Governing*

H&M’s broad definition of tools of government (Nodality, Authority, Treasure, Organization, or “NATO”) responds to two primary needs: the first is to include the different ways of use shaped in different political and cultural domains. The second derives from the first and is the possibility to make comparisons in time and among the different forms of government (p. 192). In terms of the digitisation processes, the authors note that, on one side, “... the government is aiming to ‘lead’ digital developments in the society at large” (p. 195). On the other, the possibility of adding the digital technologies to the existing toolkit varies according to the level of digitisation and digital knowledge in the society, for which the governments can follow or accelerate the pace (p. 193).

This precise definition is prerequisite because excessive misalignment—i.e., one that greatly anticipates the effective take-up level of digital skills—tends to overestimate the potentially positive effects of public leadership on de-bureaucratisation and the participation and empowerment of the citizens.

Conversely, the conditions of alignment of the governmental action with the social patterns are maintained constantly, and it can be reasonably expected that the digital age will produce its effects in terms of the ‘sharpening of the government’s tools’

(p. 196). In this respect, the authors claim that a government that sets as its goal a limited intrusion into the lives and business of its interlocutors will prefer, where possible, to use the tools of ‘nodality’ and ‘treasure’ as opposed to those of ‘authority’ and ‘organization’ (p. 196). A government “will generally aim to maximize the precision and scalability of its detecting and effecting tools, so that it hits only its intended targets and hits them only as hard as they need to be hit to achieve the desired effect” (ibid.).

Hood and Margetts point out that digitisation allows governments to extend scalability and directness. The former is the capacity to use the effectors at variable degrees of intensity. The second is the ability to tailor the effectors to specific categories of interlocutors that the government intends to engage in either positive or negative terms without triggering spillover effects (ibid.). Below, we provide some examples for each of the four tools identified by the authors.

Nodality This tool allows the government to ‘detect’ relevant information to get an overall picture and to intervene in “softer” and less costly ways than those employed by more traditional tools. For example, the analysis of traffic records in the telephony networks and online channels can generate potentially useful information flows. Likewise, the web-based technologies have strengthened the ability of governments to provide personalised messages directed at specific groups of recipients (p. 42). However, the positive aspects, such as the ability to conduct cheaper direct surveys, are accompanied by negative aspects, including the de facto exclusion of the more disadvantaged categories, such as the poor, the vulnerable, the elderly, and the marginalised. The internet age makes nodality-based tools sharper while making others less efficacious (p. 41). In definitive, the nodality of government “will depend upon government’s ability to compete successfully in the online space, something that many governments find challenging” [14].

Authority The ability to command and veto and to command and permit is exercised through the so-called ‘tokens of authority’ that are ubiquitous, both in the gathering of information and in the changing of behaviours (p. 50). These tokens translate into “[o]rders, bans, requisitions, vouchers, warrants, coupons, licences, quotas, certificates (digital or otherwise)—once you start looking, you see them everywhere.” (ibid.). And so, also in this macro-tool environment, digital technology has led to changes in both the tokens used and their degree of usage. Internet influences government’s ability to wield authority, both in terms of how citizens use the Internet to challenge or circumvent authority, and how governments use the Internet and related technologies to respond. On the other hand, the new business models and the activities developed via internet are technically hard to ‘detect’ (and, therefore, to ‘effect’) also by those governments with the required resources. Like nodality, the digital technologies also enable the authority to accurately target the interventions (the tokens) to the different categories of interlocutors (p. 72).

Treasure Like the ‘authority tokens’, the government uses the ‘fungible chattels’ it has at its disposal to gather information and to promote or discourage certain behaviours. Such examples (see pp. 78 and following) include tax rebates, public procurement, and grants to incentivise businesses to set up in certain locations. The digital age amplifies the possibilities for government to become a customer of the

private companies that produce the e-government tools, platforms and services. The digital age facilitates the implementation of specific incentivising or non-incentivising actions, as well as increasing its ability for group-targeting to encourage behaviours deemed virtuous (p. 97). Treasure was, not by chance, the earliest resource to move online from the 1950s onward.

Organization Organization denotes the entire stock of tangible and intangible resources the user has at their disposal to carry out detecting and effecting activities. According to H&M, of all the NATO tools, organization has brought the most change to the digital age (p. 119). The greatest impact underlined by the scholars is, not surprisingly, labour saving and the increasingly manifest use of intellectual capital and equipment since the early twenty-first century. Basically, the new digital technologies allow the public resources to be used in a more precise and discriminating manner than the “previously ‘unintelligent’ forms of physical effectors such as walls and barriers” (p. 120).

In short, the technological advances do not change the actual content of the government toolbox and, in a digital age as any other, the fundamentals remain “nodality-authority-treasure-organization” (p. 181). Instead, the changes triggered by the digital age affect the costs and practicality of different modes of action. In particular, the most visible effects can be seen in the information-gathering tools available to government, for instance, with the near-universal ownership of mobile phones. Hence, it is the detector that has changed more than the effector part of the operation (p. 182).

4.2 *Digital Technologies that Govern*

As outlined in §2.2 above, Hildebrandt favours a relational conception of technologies. This same view is transposed into law. In the words of MH:

A relational conception of law sees law neither as instrumentalist nor as autonomous. First, it denies that law is a mere instrument, because its instrumentality depends on the legal subject that enacts, administers or adjudicates the law, and on the ends it aims to achieve. Second, it denies that law is independent from its societal, scientific and professional environment, because its existence depends on the performative nature of the social fabric it constitutes and by which it is constituted. The latter indicates that in so far as this social fabric is articulated by means of particular ICIs, the mode of existence of the law co-depends on the ICIs that institute the society it aims to regulate (p. 172).

In addition to the impossibility of considering digital technology, as it is being developed today, neutral to policy objectives, three important consequences ensue from the inseparable interweave of society, law and ICIs. The first is that the conscious ability to deliberate is conditioned by the digital *unconscious*. The second is that the affordances of the online world lead to an instrumentalisation of the law (meaning that the technical regulation ends up supplanting the legal regulation). The third is that the ‘pre-emptive computing’ takes on a deterministic nature (pp. 184–185). To better understand the relevance of these concepts, it is necessary to delve deeper.

Conditioning the ability to deliberate The critical characteristic of the law, in addition to being binding, is that it is based on a long and careful consideration or discussion. Interaction with smart technologies creates a situation of ‘rushing to judgment’, reducing the need to stop and think about what we are doing and discouraging the thought process that delays judgement until we have considered different views or positions that counter the initial arguments. The result is a reduced capacity to deliberate (p. 184).

Instrumentalisation of the law The reduced capacity to deliberate may lead people to see the law as merely a tool to influence social actors. If the design and engineering of the digital world, inasmuch as it is unconscious-oriented, are directed at achieving policy goals to replace the legal precepts in all those cases in which the law is deemed less efficacious and less efficient, then the meaning of the law is hollowed out. The law thus becomes a tool like any other, used or not according to preferences. The question then becomes: but of which actors? (p. 185).

Deterministic effects of the ICIs Even if we deny the deterministic nature of the technology, we cannot deny that the ICIs shape the human action to a certain extent. As indicated above, this is precisely what happens when the law is perverted. With the growth of a deterministic ICI “the online world becomes saturated with invisible detection and decision mechanisms that manage to redress our behaviours instead of addressing us with regard to our actions (ibid.).

MH clarifies that the intention is not to anthropomorphize the ICIs and excludes attributing them with the capacity of agency. Rather, the point the author is making is the need to for us to condition this ‘data driven agency’ and to not let it condition us: “It is up to us to design and engineer this mind in a way that does not pre-empt us such that we become the cognitive resource of the ICI instead of the other way round” (p. 185).

For MH, the push to intervene on the ICI in the design phase is based on the fundamental right to privacy, which consists of freedom from illegal interference as a prerequisite for the freedom to develop one’s own identity (p. 189). Hence, we are talking about a design inspired by the EU’s General Data Protection Regulation (GDPR), which at the time of Hildebrandt’s writing (2015) was still in the proposal stage but was later approved in 2018. The author’s orientation is based on Legal Protection by Design (LPbD) and on Data Protection by Design, the meaning of which is basically: “LPbD seeks a methodology capable of translating legal conditions into technical requirements, taking into account the fundamental requirements of ‘resistability’ and contestability.” (p. 218). Is this perhaps a question of techno-regulation? “On the contrary, designing legal protection into an ICI means that mechanisms to steer people into certain behaviours must be made *visible* and *contestable*.” (p. 219, our emphasis).

Hildebrandt envisaged that this perspective would generate the following consequences. First, data-driven systems “will force existing technology developers to include a new set of requirements at the *starting point of their design process*, while at the same time creating a market for new technologies that help to render data processing systems compatible with the GDPR” (p. 221, our emphasis). But that is no simple task: “The challenge of translating these rights into technical and

organizational requirements is intimidating”. However, if opportunely promoted and supported by appropriate human machine interfacing technologies, the solution may lead to user empowerment.

Second, MH suggests developing counter-profiling tools and skills with respect to data-driven agency. Counter-profiling must not be confused with anti-profiling (p. 223). Hence, “At this moment there is no legal obligation to provide the socio-technical infrastructure for counter-profiling, whereas this seems to be a critical requirement for achieving the compensation that is called for by technology neutral law. The importance of such an infrastructure for the ICI of pre-emptive computing can hardly be overstated To figure out how to actually fabricate smart technologies that enable counter-profiling is no mean feat” (ibid.).

5 Discussion and Policy Implications

The foregoing discussion offers valuable ideas for interpreting and assessing current and foreseeable developments of the intertwining of society and technology. The two books reviewed address similar yet different points that we cannot go into here due to space limitations, which is why we have narrowed our focus to a selected set of issues. Nevertheless, drawing on both works together helps us to make sense of the complexity of the contemporary digital landscape.

The response to the guiding question posited at the beginning of the article—*In what way do the different ways of conceptualizing the intertwining of society and technology contribute to the practice of government in the digital age?*—can be articulated in three points.

First, it is now accepted that the ICT artefacts and their use in the government machinery and in society offer great promise but pose new challenges in reshaping government-society connections. In the words of Henman, ICTs “are part of the complex mix which defines our social realities and its dynamics” [15:19]. Nevertheless, it is one thing to acknowledge the organisational and societal relevance of ICT, but another to identify *the* source of an autonomous rationality, i.e., capable of providing universal “plug-and-play” solutions, in the potential impact of the technologies. In other words, it is illusory and misleading to treat ICT in isolation, i.e., as a variable divorced from the context, also when viewed through the lens of soft determinism, as in the case of H&M.

Second, to develop an adequate understanding of the potential of the relevant ICT tools and applications, it is necessary to consider their variety and diversity. For example, the category of social media technologies comprises “a conglomeration of web-based technologies and services” that vary dramatically in their purposes and approaches [11]. Further, their affordances, or ‘action possibilities’ [5] can be the conscious or unconscious fruit of design choices.

Third, ICT is in need of political attention. The ability of the technologies to regulate is inherently political: technology can be designed (consciously or unconsciously) to open certain social options and close others [2]. The transformative

effects move faster than the policy-making process [8]. Further complicating matters is the fact that the socio-technical nature of the change makes it unpredictable, while the intertwining of society and technology excludes the possibility of implementing ‘straightforward solutions’ [16].

The above response pulls techno-regulation away from the streamlined vision of law held by the mainstream. Many public policies date back to the pre-digital era and the difficulty of comprehending the changes underway may delay the review and adaptation of old policies [8]. Information policies can come from a large number of sources, including legislations, regulations, norms, circulars and recommendations. Italy, for example, has had a regulatory compass for its e-government policies and machinery since 2005, when the Codice dell’amministrazione digitale (CAD), or the Digital Administration Law, came into effect. Basically, CAD aggregates the norms in a similar way to the Austrian law that allows the federal government to define standard products in the ICT field [17]. In general, the law primarily gives principles and guidance in areas such as safety, trust, security, ownership rights, archiving and record keeping, but fails to address crucial issues related to human agency, equity, democracy, inclusion, equal access, etc.

The critical importance of resolving such unanswered questions, and the potential risks that stem from the excess of power wielded by the digital giants, was confirmed by a journal article [11] on the USA context: “By adopting the use of specific social media tools, government agencies appear to be tacitly endorsing the privacy, security, and other policies employed by those social media providers as adequate”. The kick in that citation is the observation that, even in an advanced country such as the USA, there is a de facto disconnect between existing information policies and the public agencies’ ongoing use of social media services.

According to a recent paper [4] on technology developments that are likely to have significant social impact in the next 10–15 years, we need better ethics for emerging technologies. Also, given the likelihood that the ICTs of tomorrow will continue to be affected by the problems of today, the public agencies must pay greater attention to information policies in their ICT-related decisions [11]. This gives policy makers the crucial task of ethically grounding the ICTs by devising an appropriate and relevant mix of regulatory framework and infrastructure.

A project funded by the European Community’s Seventh Framework Programme (FP7/2007–2013) concludes that such a framework should cover at least the following three main areas of policy activity [4:152–3]:

- (a) *Provide regulatory framework* to: support ethical impact assessment for ICTs and e-government. A techno-ethic regulatory framework would help to both raise awareness and identify and address ethical issues.
- (b) *Set up an ICT ethics observatory* in order to: provide a community-owned publicly accessible repository and dissemination tool of research on ICT ethics; give examples of approaches and governance structures that allow the addressing of ethical issues; disseminate past and current research ethics and ICT including relevant work packages and deliverables and relevant National Ethics Committee opinions.

- (c) *Establish a forum for stakeholder involvement* to: allow and encourage civil society and its representations, industry, and other stakeholders to exchange ideas and express their views. For example, policy consultation by responsibility ethics can take place in the preparatory phase of legislation relevant to technology [7] or in the software development phase.

6 Final Remarks

Guided by the ‘tools of government approach’ and the ‘data-driven agency approach’, this paper has explored concisely some of the crucial issues for the information policy design and implementation process. The relatively institution-free approach of the ‘tools of government approach’ can lead to a more nuanced vision of the digital tools available to government. It also underlines the governments’ capacity to use the tools the ‘data-driven agency approach’ helps to capture and comprehend not only the current technological developments by going beyond appearances, but also the complexity of the social impacts of the digital age.

Drawing on the combined insights of both lenses can help to upgrade existing axioms and chart the ethically best way forward. The review of a selected set of contributions (a limitation of this study) strongly implies that the change underway requires a change in pace and tack that the public decision-makers need to be alert to. The paper also has outlined how the ensuing tentative recommendations can aid the development of more responsible and integrated information policies.

Further, to deny the neutrality of the technology does not necessarily mean that the effects of the ICT will be always ethically relevant [5]. Importantly, the ethical or regulatory concerns posed by most developments (for example, in the area of artificial intelligence) are not markedly different from those posed by existing IT solutions [18].

In definitive, as Grunwald rightly observes, in the digital era it is necessary to know how to distinguish [19] between ‘business as usual’ and the need for ethically-informed reflection. In countries with a legalistic tradition, like Italy, a potential risk that needs to be addressed is to avoid dealing with the ethical concerns by force-feeding society with, yet again, a further mishmash of normative measures—that would be like “jumping from the frying pan into the fire”.

References

1. Grunwald, A. (1999). Technology assessment or ethics of technology? *Ethical Perspectives*, 6(2), 170–182.
2. MacKenzie, D., & Wajcman, J. (1999). *The social shaping of technology*. Buckingham: Open University Press.
3. Bannister, F., & Connolly, R. (2014). ICT, public values and transformative government: a framework and programme for research. *Government Information Quarterly*, 31(1), 119–128.

4. Stahl, B. C. (2011). IT for a better future: how to integrate ethics, politics and innovation. *Journal of Information, Communication Ethics in Society*, 9(3), 140–156.
5. Leenes, R. (2011). Framing techno-regulation: an exploration of state and non-state regulation by technology. *Legisprudence*, 5(2), 143–170.
6. Hood, C. C., & Margetts, H. Z. (2007). *The tools of government in the digital age*. Basingstoke: Palgrave Macmillan.
7. Grunwald, A. (2011). Responsible innovation: Bringing together technology assessment, applied ethics, and STS research. *Enterprise Work Innovation Studies*, 31, 10–19.
8. OECD, “Vectors of digital transformation,” in “OECD Digital Economy Papers,” 2019, Available: <https://www.oecd-ilibrary.org/content/paper/5ade2bba-en>.
9. Stahl, B. C., et al. (2010). Identifying the ethics of emerging information and communication technologies: an essay on issues, concepts and method. *International Journal of Technoethics*, 1(4), 20–38.
10. Hildebrandt, M. (2015). *Smart technologies and the end(s) of law*. Cheltenham: Edward Elgar.
11. Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of policies on government social media usage: Issues, challenges, and recommendations. *Government Information Quarterly*, 29(1), 30–40.
12. Hood, C. (1983). *The tools of government*. London: Macmillan.
13. Leonardi, P. M., & Barley, S. R. (2008). Materiality and change: Challenges to building better theory about technology and organizing. *Information and Organization*, 18(3), 159–176.
14. Margetts, H. (2009). The Internet and Public Policy. *Policy and Internet*, 1(1), 1–21.
15. Henman, P. (2010). *Governing electronically*. Basingstoke: Palgrave Macmillan.
16. de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: the need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), 1–7.
17. Pollitt, C. (2013). *Governments for the future*. Main Report. Helsinki: Ministry of Finance.
18. Renda A. (2019). *Artificial Intelligence. Ethics, governance and policy challenges*. Brussels: CEPS
19. Grunwald, A. (2000). Against over-estimating the role of ethics in technology development. *Science Engineering Ethics*, 6(2), 181–196.