



Responsible innovation at work: gamification, public engagement, and privacy by design

Daniele Ruggiu, Vincent Blok, Christopher Coenen, Christos Kalloniatis, Angeliki Kitsiou, Aikaterini-Georgia Mavroeidi, Simone Milani & Andrea Sitzia

To cite this article: Daniele Ruggiu, Vincent Blok, Christopher Coenen, Christos Kalloniatis, Angeliki Kitsiou, Aikaterini-Georgia Mavroeidi, Simone Milani & Andrea Sitzia (2022): Responsible innovation at work: gamification, public engagement, and privacy by design, Journal of Responsible Innovation, DOI: [10.1080/23299460.2022.2076985](https://doi.org/10.1080/23299460.2022.2076985)

To link to this article: <https://doi.org/10.1080/23299460.2022.2076985>



© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 24 Jun 2022.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)

Responsible innovation at work: gamification, public engagement, and privacy by design

Daniele Ruggiu^a, Vincent Blok ^b, Christopher Coenen ^c, Christos Kalloniatis^a, Angeliki Kitsiou^a, Aikaterini-Georgia Mavroei^a, Simone Milani^d and Andrea Sitzia^d

^aUniversity of Padova, Padova, Italy; ^bWageningen University, Wageningen, Netherlands; ^cKarlsruhe Institute of Technology, Karlsruhe, Germany; ^dUniversity of the Aegean, Aegean, Greece

ABSTRACT

Public engagement is crucial to strengthen responsibility frameworks in highly innovative contexts, including as part of business organisations. One particular innovation that calls for public engagement is gamification. Gamification fosters changes in working practices to improve the organisation, efficiency and productivity of a business by introducing gratification and engagement mechanisms in non-gaming contexts. Gamification modifies the workforce's perception of constraints and stimulates the voluntary assumption of best practices to the benefit of employees and enterprises alike. Here, we broadly discuss the use of gamification at work. Indeed, gamification raises several concerns about privacy, due to the massive collection, storage and processing of data, and about the freedom of employees: as the level of data protection decreases, so too does workers' self-determination. We argue that the implementation of privacy by design can not only strengthen autonomy via data protection but also develop more viable instances of RRI in accordance with human rights.

ARTICLE HISTORY



Received 11 November 2020
Accepted 6 May 2022

KEYWORDS

Gamification; responsible research and innovation; public engagement; privacy by design; workplace innovation; human rights

Introduction

Gamification innovations represent a quiet revolution in the organisation and management of work environments in which gratification and engagement mechanisms (comparable to those in videogames¹) are introduced in non-gaming workplace contexts² (Deterding et al. 2011). Serious games are concerned with the use of gaming for purposes other than mere entertainment or fun and have 'a special power to motivate and instruct,' thus becoming an excellent tool for easy and quick learning (Meadows 1999, 345). Because of this 'learning by doing' (Dewey 1916), gamification is particularly useful in non-ludic contexts. Game elements – including avatars, challenges, competitions, leaderboards, notifications, user profiles and role-playing – are being implemented across a wide range of sectors such as healthcare, marketing, finance, education, logistics, e-commerce and retailing. Several different organisations deploy gamification to enhance efficiency and productivity by stimulating their workers or other stakeholders (patients,

CONTACT Daniele Ruggiu  daniele.ruggiu@unipd.it  University of Padova, Padova, Italy

© 2022 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

teachers, students, clients etc.) to adopt a given desired behaviour without explicitly forcing it and to respond to anticipated problems according to their interaction with the game (Mavroeidi, Kitsiou, and Kalloniatis 2020).

In business, game design elements are increasingly being used to create more attractive work environments, capture user motivation and engagement, increase worker competence, train employees and foster best practices while avoiding the application of traditional rules and disciplinary sanctions (Mavroeidi, Kitsiou, and Kalloniatis 2019; Warmelink et al. 2020). Game design elements have been used, for instance, to train surgeons to 'heighten the awareness of all aspects of thoracic surgical education' in a more stimulating format (Mokadam et al. 2015, 1053) and to provide 'an active learning and training environment for military jet pilots' in flight simulators (Noh 2020). Alibaba introduced game design elements in its digital wallet Alipay so 'users get points through responsible use of Alibaba fintech offerings.'³ Digital games that incorporate sustainability issues have been used in education to update the competences of schoolteachers, students, who learn how to develop such digital games, and children, who learn the value of sustainability (Nordby et al. 2016). Apart from these interesting cases, gamification also raises some concerns, depending on the context.⁴

Amazon is also experimenting with using game design elements in low-skilled work. It employs them to reduce the negative experiences associated with repetitive tasks such as taking items from shelves and stowing products on them. Employees engage in a 'racing' game to fulfil customer orders while their progress is registered in a videogame format (Bensinger 2019). Workstations display staff progress in the game on small screens: lights indicate which item the worker/player needs to put in a given bin and scanning devices track task completion. Individuals, teams or entire floors can then be entered in these race-style competitions to pick or stow toys, cell phone cases, coffee makers, etc. As the game progresses, employees are then rewarded with points, virtual badges and other goodies at the end of their shift. This boosts employee engagement in the task at hand and encourages adherence to standard organisational practices. This profound ability to transform staff motivation and habits – and its potential to encompass other key stakeholders – makes the innovation of gamification a particular case of innovation that calls for a responsible innovation⁵ framework.

However, despite increases in productivity, efficiency and staff motivation, especially in contexts where there is a need to perform particularly repetitive and stressful tasks (e.g. in logistics, e-commerce, retailing and sharing economy sectors such as ride-hailing, food delivery, couriers, taxis etc.), innovations in workplace gamification can raise social and ethical issues. In more industrialised contexts, in fact, game design elements raise questions regarding health and autonomy,⁶ for example, since workers are steered into doing what they probably would not have done spontaneously of their own accord, with consequences for their health that can be relevant. Moreover, this effect is reached through a severe diminution of privacy safeguards since the introduction of gaming elements requires pervasive collection, storage and processing of employee data (Mavroeidi, Kitsiou, and Kalloniatis 2019).

This point puts employee subjectivity in sharp relief in contexts where game design elements push workers to reach higher performance levels by alleviating the tedious and stressful nature of their tasks. In this way, game design elements function as a form of human enhancement both physically (since the worker's performance is

enhanced) and morally (since the worker's motivation is modified – Perryer et al. 2016). In an analysis of 'human enhancement' in work contexts, Pustovrh, Mali, and Arnaldi (2018) argue that cognitive enhancement (pharmaceutical in their case) can raise work norms and create the conditions for work to respond to ever more stressful and fatiguing demands.⁷ Responsibility is therefore needed in managing this efficiency and effectiveness and the augmentation of bodily capacities to prolong this optimised productive behaviour over time. Gamification here becomes the main means of reaching this aim.

In this context, however, since game design elements require data to function, the process of altering worker's preferences requires a massive collection of employee data. There therefore exists a *special link* between the data that are required by game design elements in work and the autonomy of the individuals whose will is altered in gamified contexts. As personal information collected during the 'game experience' is processed through automated profiling templates (the evaluation logic and psychological induction mechanisms of which remain opaque and outside the control of the individual), the question of transparency becomes a problem of individual self-determination versus organisational conformity.⁸ Since workers are led to increase their performance in more demanding tasks which they probably would not have done spontaneously considering their repetitive and stressful nature, in the end they are induced to wish what the employer wants and completely adhere to the purposes of the enterprise. Viewed from this perspective, gamification almost represents a devious form of instrumentalisation of workers making them subject to employer demands. Therefore, through the use of game design elements and their consequences in terms of ludopathy and gaming addiction (Griffiths and Alex 2009), the transformation of staff motivation leads to employee subjectivity overlapping with that of the employer. In this context, the aims of the enterprise and workers therefore tend to coincide.

Considering their potential impact on data protection, health and autonomy rights,⁹ gamification innovations may therefore stray onto a collision course with individual rights,¹⁰ leading to them being assessable as irresponsible innovation (von Schomberg 2013).

This study does not reject gamification in the workplace as such, but questions which design requirements should be in place to meet the requirements of RRI and PbD (D'Acquisto and Naldi 2017). We do not merely critique gamified experiences that raise concerns but try to indicate the necessary correctives to make these experiences ethically sound and responsible. We intend to show that the principle of PbD can encourage responsible innovations in gamification, i.e. ones providing the desired productivity increases in an organisation while at the same time safeguarding the rights of its employees. Furthermore, we hypothesise that PbD-led responsible innovation can strengthen both data protection and autonomy in work environments.

This study is structured as follows. First, a case of game design elements in the workplace is presented that raises concerns from a RRI perspective, in particular regarding worker privacy, health and autonomy, which are considered from the legal standpoint in the following sections. To analyse the case, the literature on RRI is reviewed following a rights-based approach and responsible innovation frameworks are applied to the case of gamification innovations to identify the social-ethical issues involved.¹¹ Next, the PbD principle is proposed as a means to operationalise RRI in gamification. Finally, the introduction of game design elements in the workplace in the light of PbD is framed,

suggesting design requirements and actions to be adopted at the design stage (or ‘RRI correctives’) which can potentially strengthen data protection in an organisation in order to also enhance workers’ autonomy and their health.

The rise of gamification in the workplace

Deterding et al. (2011) define gamification as the implementation of game elements in services which are not games. electing ‘points’ to pass ‘levels’ and winning ‘rewards’ are examples of game elements (Cafazzo et al. 2012). Gamification offers benefits in several domains. In education, users’ interest in learning is increased (Lucassen and Jansen 2014), while gamification is used in logistic activities to maintain workers’ motivation (Hense et al. 2014). Apart from these domains, interactive elements have been integrated in the working environment to enhance user engagement and adoption of the services involved. Additionally, gamification affects users’ behaviour, as in some domains users have to complete their tasks to win badges (Mavroei, Kitsiou, and Kaloniatis 2019; AlMarshedi et al. 2017).

Gamification is used extensively in workplaces and results in various benefits, as it can be a solution to numerous work challenges in an organisation, including training and skill development (Ruhi 2015). Crucially, through game-like processes a productive and healthy work environment is maintained in which repetitive tasks become enjoyable. By enhancing employees’ willingness to complete such tasks, their workplace stress can be more effectively controlled, resulting in higher levels of staff health and wellbeing (Herzig, Ameling, and Schill 2012).

According to Oprescu, Jones, and Katsikitis (2014), ten principles can be applied to transform work activities through gamification. These are summarised in the mnemonic ‘I play at work.’ Taking each in turn, the ‘persuasive elements’ of gamification increase employee’s satisfaction with their work, while ‘learning orientation’ refers to the development of personal and organisational capabilities and resources. The ‘achievement-based rewards’ principle, meanwhile, boosts employee retention. The ‘Y-generation adaptable’ principle focuses on work experiences that are enjoyable and rewarding for the staff involved. ‘Amusement factors’ result in personal satisfaction. Similarly, the ‘transformative’ and ‘wellbeing oriented’ principles refer to enhanced levels of productivity and personal/organisational wellbeing respectively. Employee self-efficacy is encompassed in the ‘orientation’ principle, while the ‘research-generating’ principle improves collaboration and understanding between managers and their teams, and decision-making processes. Finally, the ‘knowledge-based’ principle refers to the systematic provision of feedback, including rewards, to employees. According to Perryer et al. (2016), when using gamified services some common issues should be considered and deserve attention, so that for using them to be effective several rules should be considered when designing them. Such rules are emphasis on cooperation to avoid negative feelings and that no further effort is required in order not to lead to demotivation. When designing services with such issues in mind, an appropriate balance between gaming and working is ensured (Perryer et al. 2016).

Gamification is variously spreading in the workplace. DevHub provides a gamified application through which employees win badges – ‘devatars’ – for completing their tasks, thus intensifying productivity, particularly among those who previously

avoided such tasks. At Google, employees who travel are encouraged to use a Travel Expense app. If they spend less than their designated expenses they are given the opportunity either to reallocate the difference to a subsequent trip, to receive it in their next pay check or to donate it to charity (Datagame 2016). Gamification can also be used to resolve organisational gaps. Lawley Insurance, for instance, designed a staff rewards contest to find and correct database inaccuracies that were leading to unreliable sales forecasts. Within two weeks, staff had hit as many of the company's targets as in the previous seven and a half months combined (Datagame 2016). Gamification also has interesting applications in the field of sustainability. The UVa Bay Game has been tested as an effective learning platform to raise awareness of sustainability issues. Students played ten two-year rounds adopting a 'doing right by doing the right thing' approach. The aim was to change their behaviour to make it more environmentally friendly (Learmonth et al. 2011).

Large-scale distribution

Despite some positive examples of applications of game design elements in the workplace (e.g. training aviators, surgeons, school teachers, students, work reorganisation in the insurance sector etc.), there are concerns regarding workplace gamification, particularly when one looks at business sectors such as logistics, e-commerce, retailing, ride-hailing, food delivery and couriers. In this case, there are specific factors related to work involving repetitive, stressful and non-provisional manual tasks, the organisation of turnover and the particular heaviness of night and day shifts that make the use of gamification problematic. In logistics, for example, packaging and order-picking tasks entail that workers have to perform the same movements for hours in day and night turns often only in contact with robots and machines. This type of work can lead to chronic diseases and various health problems concerning tendons and muscles in the workers' arms and legs, especially when a shift lasts the whole week (Ferro 2021). This aspect of work processes can change the impact of game design elements in the workplace. As ILO (2021, 220) highlights, 'gamification schemes [...] push workers towards excessively long hours and high-intensity work could be considered injurious to health.' Using gamification techniques in such work processes sheds light on more general aspects of gamification that are less visible in training settings.

Special attention must be devoted to the game case since playing is essentially opposed to working. Playing has specific relevance in human life since it allows forms of constraints typical of working to be interrupted, thus enriching the individual's imagination. While games are not the free play of imagination but quite the opposite since they follow rules, playing is fundamentally different to working. Although in an ordered form,¹² play is a key element of what in Marxist terms can be called the realm of freedom, as opposed to the realm of necessity. *Homo ludens* cannot be at the same time *homo faber*. Play in the service of work aims and with the ultimate goal of profit-making must be seen as a perversion of play when looked at from the perspective of approaches ranging from Friedrich Schiller's 'On the Aesthetic Education of Man' (1794) to Huizinga (1998). In this sense, gamification only transforms the recreative goal of playing into a means for better performing mandatory work tasks. This is a kind of trick or illusion that has consequences for workers.

Gamifying repetitive mechanical work may therefore be seen as an abuse of the human drive to play, a form of instrumentalisation of human beings and so a violation of their autonomy. As Schiller said, man only plays when he is in the fullest sense of the word a human being, and he is only fully a human being when he plays. Moreover, practically speaking, game addiction, ludopathy and a state of permanent competition with other colleagues accompanied with a perception of no constriction in performing heavy tasks can further increase pressure on employees from both the physical and psychological standpoints (Griffiths and Alex 2009).

Recently, the media have highlighted the case of Amazon warehouses, where some forms of gamification have been experimented with for a while (Bensinger 2019). This new form of labour organisation is especially relevant in the European context, in particular in terms of autonomy, health and data protection (on this, see § 4). Therefore, it is crucial to assess its sustainability given the rights system implemented in Europe¹³ and to see how it can be transformed in a way which might be compatible with European rights regulation. In other words, it should be seen whether gamification can lead to responsible and ethical outcomes (Warmelink et al. 2020).

Despite much attention by mass media, not much is known about the gamification practices in Amazon warehouses (no video or pictures are available as the use of mobile phones is not allowed). Nonetheless, information available from traditional media allows us to understand the real dimension of the phenomenon.

In 2019, Amazon started to gamify tasks in some of its warehouses to boost employees' motivation when picking and stowing items, often for ten hours a day or more (Bensinger 2019). In line with the burgeoning automation of work processes, the Amazon workforce was forced to be isolated from other workmates, to often be stationary and to perform highly repetitive tasks in situ. The use of robots flanking humans has certainly made the work less strenuous since employees no longer have to run kilometres during their shifts. However, the trade-off is a more monotonous work pattern.

To enhance the workers' productivity and make their tasks more enjoyable – or perhaps, in fact, endurable – Amazon has therefore introduced a form of gamified re-organisation of logistic work (Warmelink et al. 2020; Delfanti 2019). Experimental games entitled MissionRacer, PicksInSpace, Dragon Duel and CastleCrafter have been implemented in five warehouses on a voluntary basis. These games feature vintage old-fashioned graphic design reminiscent of videogame masterpieces such as Donkey Kong and Pac-Man. The games are displayed on small screens of workstations, like a form of workplace Tetris, and indicate which item must be placed in a given bin. Through the use of scanning devices and a tracking system for items (Delfanti 2019), individuals, teams and even entire floors can follow the progress of the work, which correlates with the completion of levels in a virtual competition. Staff are then awarded points, rewards, virtual prizes or virtual badges based on their standing on the leaderboard in the style of arcade machines popular in the 1980s. Thanks to the engaging play element associated with video games, workers perceive lower levels of fatigue and stress (Griffiths and Alex 2009) and are more motivated to follow standard protocol in less time. Anonymous workers interviewed by the *Washington Post* stated that they were able to stow up to 500 items in less than an hour. Other interviewees, also anonymously, voiced appreciation of this gamification as a means of breaking the monotony of their tasks at work.

Clearly, the redefinition of work via gamification provides significant benefits in organisational efficiency and productivity. The need for complete automation of work is avoided (Casilli 2020) while maintaining the better competence of humans with the same efficiency as machines but at a cheaper cost and with comparable outcomes (Warmelink et al. 2020). In this light, gamification leads to better integration of human labour with automatised work owing to a clear amelioration of workforce performance. Working in an artificial and permanent state of competition, employees are motivated to reach greater outcomes (Warmelink et al. 2020).

For the record, Amazon has emphasised that no employee was compelled to take part in the Palo Alto experiment and that the workers who chose not to engage in gamification processes have not been monitored or penalised (Bensinger 2019). However, a monitoring system was created following workers' participation in the gamification experiment. Moreover, given the generally accepted system of monitoring to evaluate the speed, efficiency and other key factors in workforce performance, it can be argued that non-participating workers are also covertly entered in competition with those taking part in the gamification experiments.

It is evident that for gamification to be successful, an efficient data collection system is needed. Game design elements only work with massive data collection. Without it they do not work.

However, health and privacy are not the only relevant concerns. Considering the effects of gamification enhancing workers' performance, their self-determination ability can also be considered to be at stake as processes of greater engagement in gaming, ludopathy, game addiction and the ability to work on workers' motivation are able to alter it (Griffiths and Alex 2009) making their work better integrable with that of machines. In this light, gamification functions like a clear form of human enhancement which modifies the work conditions of employees both physically and psychologically (Perryer et al. 2016). The powerful human drive to play, to use Schiller's notion, is used to turn work into play, allowing humans to better 'function' in algorithmically controlled work processes in which humans are attached to machines in new ways. This leads to a reinterpretation of the man/machine relationship within the enterprise.

Coming back to the ongoing process of automatisisation in Palo Alto, a recent analysis of patents owned by Amazon noted that 'workers are not about to disappear from the warehouse floor' (Delfanti and Frey 2020). Seen in this light, gamification can be understood as the other side of the process of automatisisation of work in the age of service digitalisation. Given the fact that introducing game design elements in the workplace pushes employees to reach a level of efficiency comparable with that of machines, workers become a competitive substitution of the process of automation. However, this outcome is only possible through persistent, selective and incisive control of data. Since gamification requires the collection, storage and processing of staff data to function properly, along with constant monitoring of their activities, systematic control of privacy appears to act as the means with which corporations can achieve total transformation of the shopfloor process. As Robinson et al. (2020) highlight, these 'opaque methods of 'algorithmic management' produce information asymmetries and surveillance that restrict workers' autonomy' and it affects their ability to develop autonomous lives (Roessler 2005) and even their identities.¹⁴ This is exactly the charge that can be levelled at gamification.

Workers' rights involved in gamification

Unlike the case of training, implementation of game design elements in large scale distribution is far from having no consequences for workers. As some noted, '[w]here they are available, bonuses have created a strong incentive structure through gamification that encourages workers to work long hours and with high intensity' (ILO 2021, 159). This surely affects their health and also their autonomy and their privacy. This worsening of their health and the large use of their data is done on a voluntary basis. What is of interest is that all these rights do not only have a moral dimension. Since they have legal recognition, from which legal obligations stem which can be linked to the norms that recognise them, they also have a legal one. Various enforcement mechanisms involving courts at the national, supranational and international levels can hinder these innovations that impact the individual rights of workers.

First, working with high intensity to perform low-skilled tasks that are laborious and repetitive puts in question the right to health in the work environment (ILO 2021, 220). This right is recognised in the constitutions of several European countries (Germany, Greece, Italy, France, Spain, the Netherlands etc.). It also has supranational recognition in the EU Charter of Fundamental Rights (art. 35) and international recognition in art. 8 of the European Convention on Human Rights (ECHR), which is supported by the jurisprudence of the European Court of Human Rights (ECtHR), from which precise obligations on States derive (e.g. *Open Door Counselling et al. v. Ireland* App. 14234/88). The right to health covers both the right to access healthcare and the right to not have any diminution of one's psycho-physical health state (Ruggiu 2018, 305 ff.). This has special relevance in the case of low-skilled works like those at the centre of some instances of gamification.

This increase in the risk to workers' health is based on a subtle modification of their motivation since the introduction of game design elements has effects comparable to human enhancement, namely to an alteration of physical performance (because their work performance is enhanced) and their psychology (because their will is altered and their attention, concentration capacity and resistance to stress are enhanced). This puts in question employees' self-determination ability.

In legal terms, workers' self-determination represents the limit of the directorial and organisational power of the employer, since it limits both the employer's power to determine work tasks (which is not unlimited) and workers' control over the execution of these tasks. According to the jurisprudence of the ECtHR, art. 8 ECHR (family and private life) protects the sphere of individual autonomy against enterprise power given the special vulnerability of workers due to the original labour asymmetry (e.g. *Copland v. the U.K.*, App. 62617/00; *Barbulescu v. Romania*, App. 61496/08, § 70). Given the special link between the determination of tasks and control over how these tasks are performed, this sphere is protected by both the 1981 Convention No. 108 (Automatic Processing of Personal Data) and the Recommendation CM/Rec 2015(5) with regard to the use of digital technology in the work environment. The latter excludes employer interference in the private life of employees (art.14) and the use of personal data not pertinent to tasks set for the work position (art. 19). On this issue, the ILO (2021, 177) notes that '[a] key facet of autonomy and control over work is related to their ability to choose working hours and break times, as well as to decline certain orders, for reasons such

as exhaustion or safety concerns.’ This means that the unbalanced relationship between an enterprise and its employees puts their autonomy in a situation of initial vulnerability, over which gamification can have effects. This is the reason why the ILO requires special attention in the case of gamification (ibid. 2021, 220).

Since the *intrinsic aim* of game design elements is to modify the individual’s motivation and this usually happens with a large collection and processing of data, within the EU the GDPR is also involved. The GDPR expressly takes employer-worker asymmetry into account since it does not consider worker consent a legal basis for processing workers’ data given their position of vulnerability (arts. 6 and 9). Data processing can be based on the enterprise’s interest in execution of the contract to which the data subject, namely the worker, is party (art. 6, 1 let. b). However, this interest is limited given the different strengths of the two parties, with the will of the employee being in a vulnerable position. In this sense, Opinion 8/2001 of the Article 29 Working Party on the processing of personal data in the employment context states that ‘[r]eliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment.’ As it modifies the employee’s motivation and this aim is achieved via data processing, gamification alters the genuineness of will. This is why data protection is essentially linked to autonomy in this context. However, this is not only because any digital technology (artificial intelligence system, chatbot, virtual assistant, software) uses data, even personal, to function, meaning that data processing by game design elements that involve workers is specifically aimed at modifying the condition of choice of the subjects, namely their will. It is also because loss of employees’ control over the sphere of self-determination starts with a parallel and pervasive loss of control over their data. In other words, the ability of gamification to foster deeper engagement by the individual (its intrinsic aim) is only achieved through collection, retention and processing of their data. Therefore, the ability to alter the individual’s motivation through gamification builds a circular connection between privacy and autonomy. In this regard, art. 88 GDPR gives States the power to adopt special measures to protect the rights and liberties of workers with regard to data processing.

If this is true, it also means, however, that if we change game design elements in a way that is privacy sound, not only can workers recover control over their data but they can interrupt the process of weakening their self-determination ability. In this sense, we believe that the assessment of gamification can change via a design approach (see § 6 and 7).

Public engagement, Responsible Research and Innovation, and RRI by design

The misalignment between workers’ privacy, health and self-determination and the employer’s interest in better work organisation, efficiency and productivity leads to the question of whether gamification is ethically acceptable and what the conditions for it to be acceptable are.

The emerging field of RRI provides useful insights to assess the ethical acceptability of innovation systems, including in the field of gamification. The Amazon case shows that the enterprise’s interest in better organisation, efficiency and productivity via the use of

game design elements can be accompanied with a sacrifice of working conditions (a state of permanent monitoring and/or competition), worsening of workers' health (a situation of psychophysical stress due to the requirement for continual human enhancement), alteration of free self-determination ability (due to game engagement, game addiction and ludopathy, which are intrinsic in gamification) and loss of workers' control over their data, which can be shared with the employer and even other colleagues. We therefore wonder if it is possible to build a responsibility framework for gamification innovations in the workplace and if so *how* (§ 7).

In the context of European policy, which aligns ethical concerns and societal interests with public investment in research and innovation, RRI has been developed as a governance framework in which 'societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products' (von Schomberg 2013, 63). This governance model aims to build a responsibility framework mainly by fostering stakeholder¹⁵ participation (inclusion) and implementing ethical acceptability in research and innovation.

Notwithstanding a large consensus on RRI at both the academic and institutional levels, two broad traditions in the RRI literature can be distinguished (Ruggiu 2015). These two traditions push RRI in two divergent directions: one towards ethical acceptability identified with *norms* set at the constitutional level; and the other towards inclusion as a *process* of public engagement. We believe that a fusion of these two traditions can be useful, not only for RRI in general but also in the case of gamification.

First, according to a normative substantial approach, the starting point of the innovation process is located in norms and values that generate products and services that serve society (von Schomberg 2013). The main characteristic of these values is that they can be identified at the level of constitutions or EU treaties (notably, arts. 2 and 3 of the Treaty on the European Union) and they aim to shape both science and innovation according to a top-down logic. Means of participation, research programmes and innovation must be anchored in shared values. Therefore, the ethical acceptability of innovation depends on values such as health, self-determination and privacy (according to an approach oriented to rights – Ruggiu 2015) and informs of what is ethically acceptable and what is not. In our case, for instance, privacy can be identified as a substantive norm that informs the gamification design process, leading to new products and services that respect the societal value of privacy. One potential drawback of this approach, however, is that values such as privacy are not monolithic. Instead, they have various levels of *application* with various consequences depending not only on the law or the way in which courts apply it. Limiting the privacy of individuals for the sake of public security, for example, differs from motives that only serve the interests of private corporations. Moreover, this approach raises questions concerning what constitutes a justifiable reason to interfere with individual autonomy and personal freedoms. In the case of gamification, the main problem would be that, on the one hand, even if privacy can be implemented top-down by the employer this might not satisfy the workers and, on the other hand, it might be insufficient to enhance their self-determination ability.

A second tradition, the procedural approach to RRI, instead focuses on the innovation *process* and the ways in which actors anticipate risks, reflect on desirable outcomes and engage stakeholders (Owen et al. 2013). In this approach, the process of

stakeholder engagement, therefore, must be open, democratic and inclusive to create ethically acceptable solutions. It is (i) a framework of responsiveness able to attract inputs stemming from society (according to a bottom-up logic) and (ii) a framework of reflexivity that leads society to collectively reflect on the purposes of innovation (Owen et al. 2013). Public engagement can be aimed at either ‘restoring trust’ in matters such as innovation where people perceive that public institutions are too far away (e.g. GMO – von Schomberg 2013) or at ‘building robustness’ to strengthen the deliberative process (Groves 2011). In general, it is required because legal responsibility schemes can be insufficient in the case of innovation (Sand 2018). In these cases, to enlarge responsibility it is necessary for all parties involved to be actively engaged through a process of responsabilisation. Ethical acceptability, namely the values needed to anchor innovation, is therefore built bottom-up *through* society, *with* society and *for* society (Owen, Macnaghten, and Stilgoe 2012). This particular process of inclusion finally generates a shared vision of societal future driving innovation in an agreed given direction (Grinbaum and Groves 2013).

In this approach, predetermined normative claims are not declared but must be identified through the inclusion of all stakeholders. Here, the emphasis is on the responsible *governance* or *management* of the innovation process, which can be achieved through stakeholder participation (Lubberink et al. 2019). In highly uncertain contexts, public engagement is the only way to establish how risks must be allocated. More specifically, potential and unexpected risks must be *anticipated* (by means of public consultations, for example), the purposes of the innovation must be *reflected* on, societal actors must be *included* and *engaged* in the innovation process, and the innovators must be *responsive* to any societal concerns raised (through forms of participation that can reach the design stage). Such concerns include the following: (a) who could be negatively affected by the gamification innovation?; (b) what is the ultimate purpose of the gamification innovation?; (c) how can employees be involved in the game design process?; and (d) what ethical concerns have to be resolved before proceeding with the innovation?

In the case of privacy, for instance, it is critical for any violations – and their harmful effects – to be anticipated throughout the innovation process. This anticipation, combined with the need for reflection, has the potential to uncover any mismatches in the innovation between the interests of employers and their employees and opens up the possibility of redesigning for greater mutual benefit. Indeed, the identification of the risks involved in gamification should be assessed not only by designers and managers (*data protection impact assessments*) but by a broader spectrum of stakeholders including, above all, workers. They must be able to choose what data can be collected, stored, and processed, with whom they are to be shared, which technical data protection measures can be implemented and what limitations are to be imposed etc. (even through forms of ‘co-design’¹⁶). The resulting responsive/responsible behaviour should engender higher levels of trust, rapport and autonomy among the various parties involved. Given that privacy is by no means a unilateral value or norm that can be implemented top-down by the entrepreneur, anticipation, reflection, inclusion and responsiveness can therefore help innovators identify the design requirements for responsible gamification.

However, it has been noted that an important drawback of this procedural approach is the fact that stakeholder inclusion and deliberation cannot wholly resolve the normative questions about ethical considerations of privacy and autonomy (Blok 2019a). In the case

of gamification, this means that even when letting workers actively participate in the process of choice in the enterprise, it cannot be ensured that the final decision taken will respect privacy. For example, in some instances of gamification workers might only adhere to the employer's desiderata and give up both their privacy and their autonomy.

Given the drawbacks of the two approaches, it has been argued that responsible management of the innovation process requires *both* predetermined substantive normative values *and* procedures, which together enhance the social desirability, ethical acceptability and sustainability of innovations (Blok 2019b). This means that, on the one hand, data protection must be ensured from the game design stage through a risk assessment of data breaches that could occur in gamification processes and through a following introduction of the necessary correctives in the design. On the other hand, workers should be allowed to actively take part in the design of all the elements that are implemented in the workplace according to a design strategy inspired by the GDPR. In other words, for a full responsabilisation of workers, it is necessary for measures implementing privacy (according to a rights-based approach) to be accompanied by measures implementing worker participation ('RRI by design'). Whereas a focus on procedures alone can lead to distortive outcomes for the enterprise (e.g. violation of rights), combining these procedural elements with predetermined tools that embed privacy requirements from the outset (i.e. by design) ensures that responsibility can be concretised at the organisational level. For this to be successful, responsible management of innovation must be implemented not only at the level of individual innovation managers and designers but equally at the strategic organisational level and the economic system level through greater engagement of employees (Long, Inigo, and Blok 2020). This action aimed at shaping the game design elements according to the proposed RRI correctives (see § 7) leads to strengthening a responsibility framework in the field of gamification. This finally leads to an integrated and embedded approach to gamification innovations in which RRI is designed in from the outset, transforming the game design elements at the design stage ('RRI by design') (Owen 2014).

The privacy by design principle

The rise of the design-thinking approach

The concept of 'RRI by design' (Owen 2014) derives from a radical mutation in the approach to innovation that finds its apex in the PbD principle. Among the several privacy strategies,¹⁷ goal-oriented approaches, risk-oriented approaches and design strategies (Hoepman 2014) ensure a deep change of perspective in gamification innovations. This is the choice made, for example, by the GDPR in Europe, and it has its roots in a long debate involving the protection of privacy in the field of ICT.

The modern-day shift from industrial manufacturing to knowledge-based economies and digital service delivery has increased the value of information and the need to manage this change responsibly (Cavoukian 2011). The PbD principle attempts to respond to this need through a change of approach to innovation from a design-thinking perspective.

In business ethics, adopting design thinking leads to a radical change in the approach to problem solving at the organisational, strategic and product-development levels of an enterprise (Brown and Katz 2009). Complex problems, such as the ‘wicked problems’ (Buchanan 1992) in gamification, must be handled contextually at the design stage of a system, which in turn requires a degree of practical foresight (Jones 1992). This implies a shift in focus from mere analysis of a problem to its contextual resolution as the starting point of the construction of the system (Nelson and Stolterman 2012), as in the case of game design elements. The use of design-thinking methodology therefore provides a framework for understanding and pursuing innovation in methods that ultimately contribute to the systematic growth of the enterprise and enhanced benefits for its clientele.

The development of privacy-enhancing technologies (PETs) towards the end of the twentieth century shifted the attention of the scientific community to the protection of individuals’ personal information (Rodotà 1995; Borking et al. 1995). In the age of big data, the human body tends to become a digital body, a fulcrum for data that transcends the corporeal (Rodotà 2016). Against this backdrop of the datafication of human life (D’Acquisto et al. 2015, 8), protection of individuals and all their data becomes a ‘wicked problem’ that must be tackled from the outset, i.e. at the design stage. Privacy must be incorporated in IT systems, design processes, organisational procedures and planning operations that may impinge on individual lives and liberties (Cavoukian 2011, 1). This leads to forms of design oriented towards the protection of rights (Ruggiu 2015). Hence, the discussion shifts from the issue of ‘big data versus privacy’ to that of ‘big data with privacy,’ according to which privacy requirements should be identified early on in the big data analytics value chain (D’Acquisto et al. 2015, 8). Privacy-enhancing measures must be built in ‘by design’ (van den Berg and Leenes 2013) which leads us to the PbD principle. This approach has been incorporated in the GDPR, which is relevant in cases of gamification applied in Europe.

The protection of privacy under the GDPR: by design and by default

Under the GDPR, PbD (art. 25), which is mandatory,¹⁸ covers both the ‘data protection by design’ (DPbD) principle and ‘data protection by default’ (DPbd), which are strictly intertwined. These two principles are functional to one another.

DPbd is characterised by a proactive approach that aims to anticipate and prevent data breaches before they materialise (Cavoukian 2011, 1). This implies first a thorough risk assessment (‘data protection impact assessment’ – art. 35 GDPR) to identify at an early stage all the possible violations of rights according to a rights-based approach (Ruggiu 2015). Rather than reacting to privacy-invasive events after the fact, privacy standards must be set and enforced at the design stage of networked data technologies. Only by having a *vision* of potential breaches is it possible to imagine the counter-measures that can be adopted at the design stage (§ 7). Therefore, PbD aims to deliver the maximum degree of privacy from the outset, ensuring that personal information is automatically protected in any IT system or practice that involves the processing of data (Cavoukian 2011, 1).

According to DPbd, instead, privacy becomes the default setting: if individuals do nothing, the system will protect their privacy and continue to do so without a need

for legal action or judicial remedy. In this sense, following the ‘DPbd’ principle, the types of data collected and/or processed must be solely those necessary to reach the predetermined purposes (‘data minimisation’ principle – art. 5 let. c GDPR) (Cavoukian 2011, 2). Moreover, GDPR also provides that ‘by default personal data are not made accessible [...] to an indefinite number of [...] persons.’ Therefore, DPbD operates in a context that is already limited by default, strengthening the technologies that are developed. This action by default is functional to the implementation of the data protection measures at the design stage of any processing system, such as game designing elements.

An example of how PbD has operated under the GDPR in Europe can be seen in the way in which cookies are handled when browsing a website in the EU, namely through the use of informative pop-ups that give all users the possibility to choose the way they want their data protected, the subjects who can access them, with whom the data can be shared, the limits of profiling and the limits of legitimate interest, etc. This would not be possible without a radical transformation *by design* of the technologies that are used to make the internet work.

The protection of data by design requires articulated and multi-level action. From the outset, PbD demands adherence to three guiding principles (Cavoukian 2011, 2). First, the purposes for which data are collected, used, retained and disclosed must be specified (‘purposes specification’) and communicated to the individual at the time of collection (art. 5 let. b GDPR). Second, the collection of personal data must be fair, lawful (‘lawfulness principle’ according to arts. 5 let. a and 6 GDPR) and limited to what is strictly necessary for the specified purposes (‘data minimisation’ – art. 5 let. c). Third, the use, retention and disclosure of personal information cannot proceed without the permission of the individual (‘consent’) except where otherwise required by law (art. 7 GDPR). These guiding principles are implemented by embedding privacy in the design and architecture of IT systems, operations and practices (Cavoukian 2011, 3) so that privacy implementation measures become an integral component of the system (rather than a reactive bolt-on) and without diminishing its overall functionality (PbD according to art. 25 GDPR). This means that in gamification contexts, workers must be well informed of the types of data, purposes of processing, the technical measures adopted, conditions for retention, durability (when the data are cancelled) and levels of protection (measures that are to be adopted). Furthermore, if the data are able to identify the subject, the worker must be put in the condition of making a real choice about them from the beginning of the development stage of the technology.

Data, however, even in the case when they can be collected and processed, do not go out of the control of the worker forever. Processing must have an end (durability). The implementation of privacy aims to accommodate all interests and objectives in a positive-sum or ‘win-win’ manner, as opposed to a more dated zero-sum approach (Cavoukian 2011, 3). This overcomes false dichotomies such as ‘privacy versus security’ by highlighting that it is far more desirable to realise both within the same framework, the composite functionality of which leads to business success. From this perspective, adopting the principles of data protection becomes ‘an essential value of big data, not only for the benefit of the individuals, but also for the very prosperity of big data analytics’ (D’Acquisto et al. 2015, 8). Equally, embedding privacy elements within an IT system must occur prior to data collection and extend securely throughout the entire life cycle of the data concerned (Gross and Acquisti 2005). The data controller, like the entrepreneur in the

workplace, must also ensure that all information is securely destroyed at the end of the process. PbD therefore produces a secure lifecycle of data from cradle to grave: security is end-to-end (Cavoukian 2011, 3). Similarly, when the game design elements are also involved, the employer must communicate to the workers how long the data are collected and processed, making the end explicit.

In this framework, it is also crucial to adopt and implement measures of a technical and organisational nature that prevent the direct or indirect identification of the individual whenever personal data¹⁹ are concerned (art. 25 GDPR). This implies that these measures must be thought of, developed and integrated in the technology by design. This is crucial in gamification innovation because the possibility of identification is the beginning of loss of control by workers and of the limitation of their autonomy (de Andrade 2011). Examples of this implementation process include the measures of anonymisation or the pseudonymisation of information collected. However, as we will see (in § 7 below), further measures must accompany data encryption measures. Anonymisation measures mean that individuals cannot be identified within a group or associated with any specific data. Instead, pseudonymisation suspends the objective link between the information and the person concerned via the use of pseudonyms, impeding the identification of the subject only temporarily (D'Acquisto and Naldi 2017, 33 ff.). However, today advances in processing techniques allow identification of the subject through accurate integration of even anonymous data. This possibility cannot be ignored when workers have to actively take part in the design of their privacy in gamification contexts.

The need of engaging stakeholders at the design stage

More broadly, PbD also seeks to ensure the inclusion of all stakeholders (pursuant to the stated promises and objectives) in a transparent and open manner. Visibility, openness and transparency concerning policies and procedures are essential for the ongoing accountability of the data controller and for stakeholders' trust in a system optimised for business success (Cavoukian 2011, 4). In this light, participation by stakeholders, like workers in cases of gamification in the workplace, can be considered a further consequence of PbD. This means that workers must be put in the situation of being able to choose not only which data can be collected by game design elements and which level of protection is to be implemented but also which type of game design elements are adopted in the workplace via forms of feedback (forms of cooperation v. forms of competition). Finally, PbD requires data controllers and designers to keep the interests, needs and concerns of their users (namely workers) at the forefront by implementing strong privacy defaults by design, appropriate and prompt communications and user-friendly and user-empowering options (Acquisti, Brandimarte, and Loewenstein 2015) and means of feedback (user-centric architecture). This definitely leads to forms of *co-design* in gamification that can be considered the end of full participation in the design stage (although not the only form of participation).

RRI correctives to game design elements in the workplace

A major challenge when using useful gamified applications is to protect employees' personal data (Mavroeidi, Kitsiou, and Kalloniatis 2019). Equally, fostering trust among

employees is of great importance in the adoption of RRI frameworks (Ruggiu 2015). Businesses must therefore pay close attention to data protection while keeping their employees informed of their privacy rights and the data management, e.g. access rights, data use (Yonemura et al. 2017). Plenty of laws, regulations and policies worldwide emphasise the importance of protecting employees' privacy in various business systems, aiming at providing a balance between collecting enterprise data and individual privacy protection (Adams 2017).

Many differences characterise these laws, for instance there is little correspondence between the United States' and the EU's fundamental rights of data protection. In the USA there are no constitutional/legal requirements for data processors on how to use personal data (Schwartz and Peifer 2017). They are nowadays expected to manage the collection, storage and usage of personal information effectively (Dinev et al. 2013). In this respect, privacy engineering in such systems is immense not only in Europe but recently also across the Atlantic. This is a significant part of the system development process, where privacy developers should define principles in the form of technical requirements that need to be satisfied in order for the system to ensure a minimum level of privacy and be trustworthy for users (Martin & Kung, 2018).

In the EU, GDPR enforcement has made the protection of personal data compulsory for all organisations during systems design and implementation (Sousa et al. 2018). New data rights have been established for EU citizens, supporting their autonomy and self-determination. Additionally, each organisation is obliged to establish a Data Protection Officer (DPO), an expert in data protection rules and practices who is responsible for ensuring that organisational processes comply with the legislation (art. 37 GDPR).

The DPO is expected to support the procedure effectively for both the business and the employees. The DPO must provide business developers with the necessary information to combine privacy by design principles with the GDPR requirements, so a strong elicitation process for the set of technical requirements that should be addressed needs to be established. He/she must propose a process for validating the elicited requirements in a data protection impact assessment (DPIA) – carried out according to the GDPR – to identify privacy risks. As far as employees are concerned, the DPO is expected to enhance their ability to trace their personal data by offering easy-to-use services raising their privacy awareness level.

This move towards transparency in data management improves trust among stakeholders (Stanculescu et al. 2016). All workplace services, including gamified ones, should be designed with the users' privacy protection in mind.

However, several game elements violate the privacy requirements, leading to violations of users' privacy (Mavroei, Kitsiou, and Kalloniatis 2019). In response, a PbD approach is suggested, considering that it has been newly incorporated in the GDPR (Romanou 2018). One key issue for the implementation of PbD is analysis of technical privacy requirements in systems during the design process. This is required in various privacy engineering methodologies (Pattakou, Kalloniatis, and Gritzalis 2017; Pattakou et al. 2018; Kalloniatis 2017; Argyropoulos et al. 2016). Among them, a privacy safeguard (PriS) (Kalloniatis, Kavakli, and Kontellis 2009; Kalloniatis, Kavakli, and Gritzalis 2007), an established PbD approach, identifies the following privacy requirements: anonymity (unknown identity of users); pseudonymity (protection of anonymity with a pseudonym); unlinkability (inability to relate subjects to actions); undetectability

(impossibility of disclosing components); and unobservability (inability to disclose actions).

These requirements have been used to prove their violation by a variety of game elements (Mavroeidi, Kitsiou, and Kalloniatis 2019), as is summarised in Figure 1. This violation occurs regarding legal issues with GDPR compliance and regarding contextual privacy expectations of users due to disclosure of their identities. The elements can be harmful or non-harmful for users’ identities (Mavroeidi, Kitsiou, and Kalloniatis 2020). Collecting points, for example, is not a harmful process, while presenting them on leaderboards assigned to user profiles results in privacy violation. As leaderboards publicly present the status of users, violation of their identities occurs.

In order to use an avatar, a record of users’ characteristics is needed, leading to violation of users’ privacy (Mavroeidi, Kitsiou, and Kalloniatis 2019). Following this approach, the relations among elements and requirements has been examined and the results are presented in Table 1. PriS considers privacy requirements to be organisational goals and describes the impact of privacy goals on the organisational processes affected. These processes aim to support the selection of a system architecture that best satisfies them. Therefore, PriS provides an integrated way of working, from high-level organisational needs to the IT systems that satisfy them (Kalloniatis, Kavakli, and Gritzalis 2008). PriS is considered in a study by Robol, Salnitri, and Giorgini (2017) to be an effective method to use in GDPR-compliant socio-technical systems. The GDPR aims (a) to promote organisations’ and companies’ data collection and processes by introducing specific privacy requirements as primary goals, thus dealing with several complex issues, such as company-level awareness (Tikkinen-Piri, Rohunen, and Markkula 2018;) and (b) to provide EU citizens with further control of their personal data while minimising threats to their data rights and freedoms (Lambrinouidakis 2018). Therefore, the conceptual association with PriS requirements is more than clear, since they promote a set of expressions based on which all the processes of an organisation are considered.

Conversely, according to the RRI framework, privacy requirements should be implemented during the design of workplace gamified services to ensure privacy protection. PriS, for instance, proposes software design patterns for the analysis of privacy

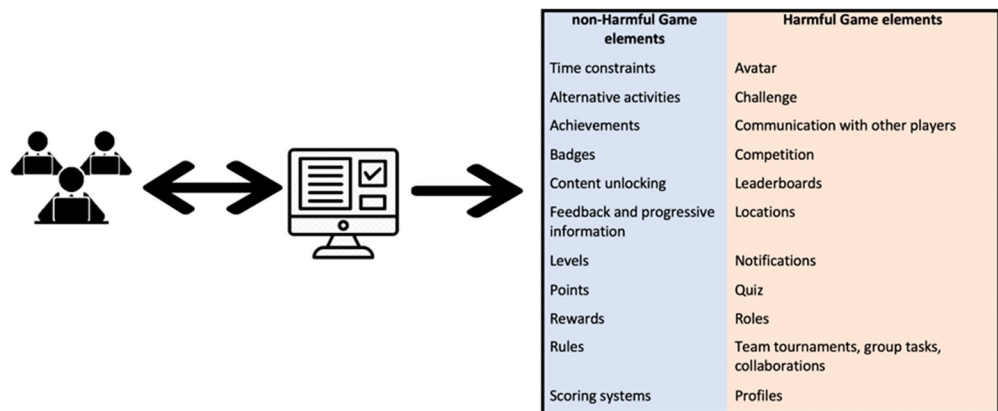


Figure 1. Categorisation of game elements.

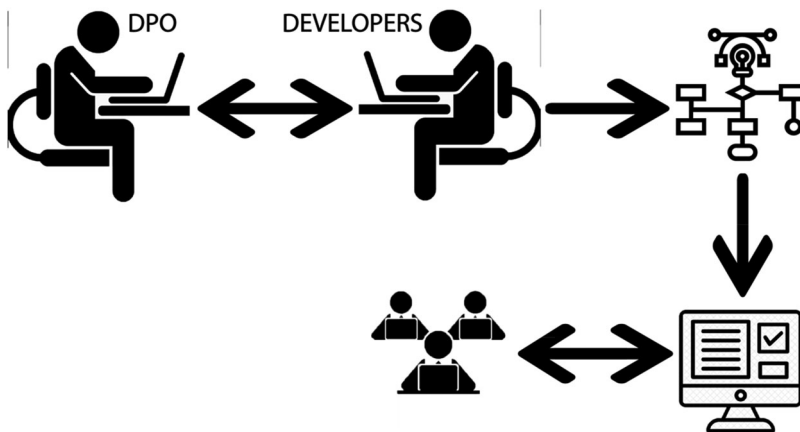
Table 1. Violations of privacy requirements.

Game elements	Violated privacy requirements
Avatar	R1, R2, R3, R4, R5
Challenge	R1, R3
Communication with other players	R1, R2, R3, R4, R5
Competition	R1, R2, R3, R4, R5
Leaderboards	R1, R2, R3
Location	R1, R2, R3, R4, R5
Notification	R1, R2, R3, R4, R5
Quiz	R1, R2, R3
Roles	R1, R2, R3, R4, R5
Team tournaments, group tasks, collaboration	R1, R2, R3, R4, R5
Profiles	R1, R2, R3, R4, R5

*R1 = Anonymity; R2 = Pseudonymity; R3 = Unlinkability; R4 = Undetectability; R5 = Unobservability.

requirements in systems (Kalloniatas, Kavakli, and Gritzalis 2007). These can be implemented when designing gamified services in order to satisfy the goals of the RRI framework regarding responsible innovation. Given the apparent privacy violations presented in Table 1, these privacy-enhancing patterns can be deployed to comply with the corresponding requirements in the initial design stage. Using the anonymity and pseudonymity pattern, at the user's request the system determines whether identity is needed and provides and implements processes depending on the case. Similarly, for the requirements of unobservability and unlinkability, the system will check a user's request to ascertain whether one or both of these requirements are necessary before connecting the user, thereby protecting user privacy.

Below we present two distinct scenarios for correctives aimed at implementing an RRI framework in a gamified workplace setting. The first scenario concerns employees' mandatory daily tasks, as presented in Figure 2. A company selling herbal beauty products has decided that its marketing team should communicate through a gamified application in the hope that the tasks assigned will be completed more promptly and efficiently, thereby increasing the company's revenue. After an effective promotion, the team member will win rewards in line with the higher profits generated. New business targets will be announced each time, which are to be accomplished in a more effective manner

**Figure 2.** Protection of employee privacy in gamified work tasks.

according to the application. Through this motivational way of working, employee productivity will be increased and workplace anxiety reduced. The employees will further embrace the company’s philosophy, as organisational objectives will interlink with their own personal goals.

However, since the purpose of the gamified workplace is to engage users in timely and efficient working, their identities should be protected. During their interactions with the application, therefore, each user’s identity will be hidden. Additionally, rewards should not be published: this is to prevent perceptions of the gamified team process as a negative challenge to workers. To achieve the objective of a departmental gamified platform that still protects employee privacy, the developers of the gamified services should consider privacy issues in parallel with game elements during the design cycle. The company DPO should support the developers by informing them which information should be protected in the game elements implemented. This will be used to determine the specific privacy requirements for the service. To this end, the DPO will provide the guidelines for a DPIA method to deploy in order to identify the likelihood of any possible privacy violation incidents deriving from the game elements (the relevant harmful game elements are presented in Table 1). Having determined the privacy requirements, the DPIA will assist in the identification and assessment of privacy risks, leading to the selection of appropriate measures to reduce them. By analysing the privacy requirements and following the PriS method, this aim will be accomplished since the appropriate technical countermeasures to satisfy each requirement will be identified. This information will allow the developers to select and proceed with the most suitable implementation techniques to ensure the protection of the users’ privacy (e.g. satisfaction of user rights etc.).

This protection, in turn, will amplify the trust between the marketing team members and the wider organisation. The employees will have a more positive attitude to their work, the atmosphere among team members will be more constructive and their managers will be gratified by a more efficient achievement of company targets.

Additionally, based on the correctives in the RRI framework, the employees should play an active role in the gamified application design process. The second scenario features this incorporation of employee preferences during system design, and is presented in Figure 3. Taking into consideration the harmful and non-harmful game elements mentioned previously, the organisation DPO informs the person responsible for the HR department about the elements. Next, this person records the elements that each employee prefers to be part of the design of the gamified application that they will be

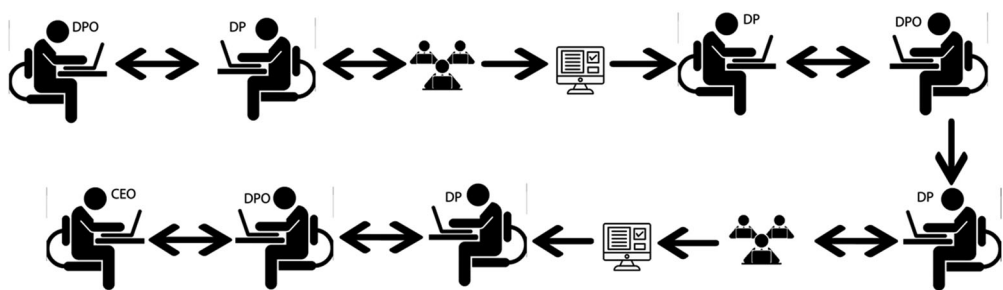


Figure 3. The employees’ role in designing gamified workplaces.

using at work. The DPO receives and collates the feedback and notifies HR of any harmful cases of privacy violation and how they can be resolved prior to rollout. This information is communicated to the employees so they remain informed about the possible consequences of these harmful elements. Specifically, employees are informed in detail about potential violation of their privacy and trained on the potential threats occurring in each harmful game element. Thus, they will be aware of every disclosure of their information.

The second phase of game element selection considers how non-harmful game elements can be used safely, while outlining the measures required in response to the harmful game elements. The list of the preferred game elements is then reported to the DPO, who will notify the CEO, highlighting the importance of privacy protection, especially during the use of harmful game elements. In this scenario, the users remain informed regarding the harmful side of gamification and are given an active role in the design of the gamified service. Their participation in the process is useful and important. By implementing these steps and including them in the design process, the workers have the opportunity to consciously select the game elements as they will be aware of possible privacy violations. This procedure will reduce the potential impact of the risks on the employees, and also the risk of non-compliance with GDPR rules at the operational level.

Introducing gamification in workplace activities can increase employee engagement and productivity regarding various organisational targets. The protection of personal data is crucial to ensure trust among staff, management and the organisation as a whole. By implementing these scenarios user privacy is protected and GDPR regulation is applied.

Conclusions

The introduction of specific forms of gamification in the workplace seems to have the same rationale as public engagement in RRI, which is that of engaging the workforce to reorientate internal practices and create overall alignment with company goals. Organisations can achieve performance, efficiency and productivity improvements while lightening the load of laborious, monotonous and stressful tasks for their employees.

However, concerns remain over the interconnected issues of employee privacy, health and autonomy, particularly given the extent to which personal data is used in gamification. When harmful, gamified activities will inevitably affect and limit the self-determination of staff, leading them to accept work conditions that can be quite demanding from the health standpoint (human enhancement in the case of non-provisional tasks). When privacy is integrated by design, on the other hand, the inclusion of data protection has the potential to strengthen autonomy. This study has demonstrated how, based on the principle of PbD, it is possible to develop the tools and systems needed to raise the level of privacy protection in gamification. Furthermore, it has suggested that full empowerment of workers requires employees to be given greater control not only over their personal data but also over the choice of the game design elements (moving towards forms of *co-design*). By adhering to an RRI model, the infringement of privacy, health and autonomy is not an unescapable outcome of gamified activities at work. Gamification can in fact lead to fully responsible outcomes.

Notes

1. Gamification can be realised both with board games (see, e.g., Chappin, Bijvoet, and Oei 2017) and with digital technologies. In this work we only focus on the case of gamification via digital technologies because it has interesting implications from the legal, informatic and governance standpoints.
2. Although game elements can be introduced across a broad spectrum of fields, such as business, education, military, traffic flow, healthcare, training, etc., in this study we focus mainly on business.
3. E.g. <https://ub.triviumchina.com/2019/06/the-gamification-of-social-values-alibaba-experiments-with-behavior-modification/>.
4. Some work environments where low-skilled tasks are carried out are more demanding for the workers from the physical standpoint (fatigue, stress, impact on health, long duration etc.). In these contexts gamification mainly alters perceptions of the impact of the tasks assigned, aggravating their consequences, especially on workers' wellness and on labour asymmetry with the employer (ILO 2021, 220).
5. Here we follow von Schomberg's definition of responsible research innovation (RRI) (von Schomberg 2013, 63). See § 6 below. However, although the present work can be traced back to his reflection on RRI focusing on public engagement and ethical acceptability as the framework for research and innovation, it will only focus on the case of responsible innovation (RI) in the field of gamification.
6. In this context, although they have a moral dimension, self-determination, health and privacy are mainly considered from the legal standpoint (see § 6 & 4).
7. This also puts workers' right to health at risk (see § 4).
8. Regarding the legal meaning of the notion of worker self-determination, see § 4.
9. On these issues, see § 6 and 4.
10. The present article focuses on the individual rights of workers in the European context, notably the rights to autonomy, health and privacy (see § 4 and 6). Apart from their moral dimension (only supported by moral obligations), these rights are only considered here from the legal standpoint. In this sense, we define individual rights as those established by a national legal order (constitutional rights), a supranational legal order (EU fundamental rights) or international law (human rights) of either the individual as such (human rights) or the citizen (constitutional and EU fundamental rights) and protected by a judicial mechanism (national courts, the Court of Justice of the European Union, the European Court of Human Rights – ECtHR). These different systems of right protection provide multiple levels of defence in the case of workers. This is relevant since litigation can hinder innovation or even make it fail. In this sense, there are possibilities of litigation over rights breaches at three levels (national, EU, international) to also protect individuals as workers.
11. The RRI literature has been reviewed privileging tendencies that consider the protection of rights to be crucial to achieve responsible and ethical outcomes.
12. Each game follows some rules of play.
13. This means mainly considering the frameworks of the Council of Europe and of the European Union.
14. On the relationship between privacy and individuals' identities, see Hildebrandt 2006 and de Andrade 2011.
15. According to stakeholder theory, a stakeholder is any centre of interest affected by business ability to raise an ethical bond for the enterprise. Therefore, stakeholders can be shareholders, funders, clients, workers, trade unions, civil society and even the environment. According to this approach, the obligations of the enterprise do not end in the legal field (legal obligations) but also cover ethical bonds identified by the group of stakeholders in a business (moral obligations). This leads to acknowledgement of the insufficiency of the mere legal dimension of business regarding the corporate social responsibility paradigm (Goodstein and Wicks 2007).

16. ‘Co-design’ is a form of innovation where the users become an active part of the innovation process in the design stage. In this framework, users therefore become innovators.
17. The concept of privacy was first known as “the right to be alone,” as in an article by Samuel Warren and Louis Brandeis (1890). However, soon with the second industrial revolution and the spread of the first cameras, two subconcepts were distinguished: the right to privacy covering the confidentiality of the life of the individual (e.g. that an individual may like to wear women’s dresses in his private life), which is strictly linked to the individual’s consent, and the right to data protection, which addresses the need to protect the integrity of data regardless of whether an individual has expressed consent (e.g. the information contained on a ticket from London to Oxford). These two dimensions, the subjective one linked to the will of the person and the objective one linked to the safety of data, are both covered by privacy and are expressed in the Charter of Fundamental Rights of the European Union in two different articles (arts. 7 and 8).
18. According to art. 83,5 lets. a and b GDPR, violation of the conditions for consent (art. 6) and the rights of the data subject can lead to a fine of €20 million or up to 4% of the total worldwide annual turnover in the preceding financial year.
19. Any data is personal when, although subjected to measures of cryptisation (anonymisation or pseudonymisation), once they are integrated with other anonymous or pseudonymous data they are able to lead to identification of the person. This functional definition of personal data also clarifies how the concept of harm must be understood under the EU regulation on privacy. In this context, ‘harm’ is any breach of the right to data protection which can lead to identification of the subject. The notion of harm also covers any infringement of a right protected at the constitutional level, EU level or international law level. Therefore, first of all privacy and data protection.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

The cost of the Open Access publication are supported by University of Padova, Department of Political Science, Law, and International Studies.

Notes on contributors

Daniele Ruggiu is Assistant Professor in Legal Philosophy at the Department of Political Science, Law, and International Studies of the University of Padova. His main focus is on the impact of new and emerging technologies on human rights, on governance models, in particular Responsible Research and Innovation, on the role of the European Convention on Human Rights in technology innovation, on the philosophical aspects of the application of law and legal hermeneutics in the Gadamer’s and Ricoeur’s perspective. Ruggiu has taken part to several projects at the national and international level (SynthEthics, Epoch project, Res-AGorA, Neurolaw Network). He has several national and international publications, in particular: *Human Rights in the Era of Emerging Technologies* (Il Mulino 2012, in Italian) and *Human Rights and Emerging Technologies: Analysis and Perspectives in Europe* (Pan Stanford Publishing, 2018, with a foreword by Roger Brownsword). Ruggiu published several articles in high ranked disciplinary journals like *Nanoethics*, *Philosophy of Management*, *Law Innovation and Technology*, *Journal of Law and Technology*, *Biotechnology Law Review*, *Rivista di Filosofia del Diritto*, *Ragion pratica*. He collaborates with *Ars interpretandi* and *Agenda digitale.eu*.

Vincent Blok is associate professor in Philosophy of Technology and Responsible Innovation at the Philosophy Group, Wageningen University (The Netherlands). He is also director of the

4TU.Ethics Graduate School in the Netherlands. Together with seven PhD candidates and four Post-docs, he reflects on the meaning of disruptive technologies (AI, Synbio, digital twins) for the human condition and its environment from a continental philosophical perspective. His books include Ernst Jünger's *Philosophy of Technology. Heidegger and the Poetics of the Anthropocene* (Routledge, 2017), *Heidegger's Concept of philosophical Method* (Routledge, 2019), *The Critique of Management. Toward a Philosophy and Ethics of Business Management* (Routledge, 2021), and *From World to Earth. Philosophical Ecology of a threatened Planet* (Boom, 2022 (in Dutch)). Blok published over hundred articles in high ranked disciplinary philosophy journals like *Environmental Values*, *Business Ethics Quarterly*, *Synthese* and *Philosophy & Technology*, and in multi-disciplinary journals like *Science*, *Journal of Cleaner Production*, *Public understanding of Science* and *Journal of Responsible Innovation*. See www.vincentblok.nl for more information about his current research.

Christopher Coenen, political scientist, works in the strongly interdisciplinary field of technology assessment at KIT's Institute of Technology Assessment and Systems Analysis (ITAS), where he heads the research group 'Life, Innovation, Health and Technology' and has carried out projects for the European Commission, the German Federal Ministry of Research and the Bundestag, among others. He is the editor-in-chief of the journal 'NanoEthics: Studies of New and Emerging Technologies'.

Dr. Christos Kalloniatis holds a PhD from the Department of Cultural Technology and Communication of the University of the Aegean, a master degree on Computer Science from the University of Essex, UK and a Bachelor degree in Informatics from Technological Educational Institute of Athens. Currently he is an Associate professor and head of the Department of Cultural Technology and Communication of the University of the Aegean and director of the Privacy Engineering and Social Informatics (PrivaSI) research laboratory. He is a member of board of the Hellenic Data Protection Authority and former member of the board of the Hellenic Authority for Communication Security and Privacy. His main research interests are the elicitation, analysis and modelling of security and privacy requirements in traditional and cloud-based systems, the analysis and modelling of forensic-enabled systems and services, Privacy Enhancing Technologies and the design of Information System Security and Privacy in Cultural Informatics. He is an author of several refereed papers in international scientific journals and conferences and has served as a visiting professor in many European Institutions. Prior to his academic career he has served at various places on the Greek public sector including the North Aegean Region and Ministry of Interior, Decentralisation and e-Governance. He is a lead-member of the Cultural Informatics research group as well as the privacy requirements research group in the Department of Cultural Technology and Communication of the University of the Aegean and has a close collaboration with the Laboratory of Information & Communication Systems Security of the University of the Aegean. He has served as a member of various development and research projects.

Dr. Angeliki Kitsiou is a post-doctoral researcher at the Department of Cultural Technology and Communication of the University of the Aegean and teaches as adjunct faculty at the same *Department*. She holds a PhD in Sociology from the University of the Aegean. Her thesis focused on the study of the Free Software Movement, highlighting the new challenges regarding deviance, social control and information management related to the Information Society. She has been involved in several funded research projects concerning innovative educational and quality assurance methods and social policy emphasis added on juvenile and immigrants. Her research interests and recent publications concern the bridging between sociological theory and privacy frameworks, associated with the most current developments in Social Sciences and Informatics.

Katerina Mavroeidi holds a BSc from the Department of Cultural Technology and Communication of the University of the Aegean and a Master degree on Cultural Informatics and Communication from the same University. She has also achieved a Master degree on Information Security from the University of Brighton. Currently, she is a PhD student at the Department of Cultural Technology and Communication of the University of the Aegean. Her skills include computer graphics and user interface design with the focus on user experience and usability evaluation.

Her second master degree broadened her knowledge on Information Security. Based on that, her skills include also analysis and modelling of security and privacy requirements, software architecture and risk management. Her dissertation of this master was about usable security. In addition, her interests lie in the area of usable privacy.

Simone Milani is Associate Professor at the Department of Information Engineering, the University of Padova., and he's currently the heading teacher for the courses Digital Forensics, Biometrics, Immersive Technologies and 3D Augmented Reality. He received the Laurea degree in telecommunication engineering and the Ph.D. degree in electronics and telecommunication engineering from the University of Padova, Padova, Italy, in 2002 and 2007, respectively. He was a Visiting Ph.D. Student with the University of California at Berkeley, Berkeley, CA, USA, in 2006, and later he worked as Post-Doctoral Researcher for the University of Udine, Udine, Italy, the University of Padova, and the Politecnico di Milano, Milan, Italy, from 2007 to 2013. He has also been consultant for STMicroelectronics, Agrate, Italy. He is member of the Ethical Committee of the Human Inspired Technologies center at the University of Padova and of the Information Forensics and Security Technical Committee of the IEEE Signal Processing Society. He's author of more than 120 papers published on international conferences and journals. His research interests include artificial intelligence and deep learning, digital signal processing, image and video coding, 3D reconstruction and rendering, Augmented/Virtual/Mixed Reality, and multimedia forensics.

Andrea Sitzia is Labour Law Associate Professor at the Department of Political, Juridical and International Studies of the University of Padova, where he currently teaches Labour Law and EU Labour Law; he also teaches Law, Informatics and Society at the Informatics degree course. He received the Laurea degree in Jurisprudence and the Ph.D. degree in Labour Law from the University of Padova. He has stable research and teaching exchanges with the Eotvos Lorand University of Budapest and with the University of Reims, Champagne-Ardenne. President of the Certification Commission of Labour contracts at the University of Padova. He's author of more than 100 papers published in national and international conferences and journals. His research interests include privacy, employer's power of control, contracts, supply chain regulation, inmates work, ILO conventions.

ORCID

Vincent Blok  <http://orcid.org/0000-0002-9086-4544>

Christopher Coenen  <http://orcid.org/0000-0002-9572-636X>

References

- Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–514.
- Adams, M. 2017. "Big Data and Individual Privacy in the Age of the Internet of Things." *Technology Innovation Management Review* 7 (4): 12–24.
- AlMarshedi, Alaa, Vanissa Wanick, Gary B. Wills, and Ashok Ranchhod. 2017. "Gamification and Behaviour." In *Gamification*, edited by Stefan Stieglitz, Christoph Lattemann, Susanne Robra-Bissantz, Rüdiger Zarnekow, and Tobias Brockmann, 19–29. Cham: Springer. doi.org/10.1007/978-3-319-45557-0_2.
- Argyropoulos, Nikolaos, Christos Kalloniatis, Haralambos Mouratidis, and Andrew Fish. 2016. "Incorporating Privacy Patterns into Semi-Automatic Business Process Derivation." In *2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS)*, edited by Sergio Espana, Jolita Ralyte, Carine Souveyet, 1–12. Grenoble: IEEE. doi.org/10.1109/RCIS.2016.7549305.
- Bensinger, Greg. May 20, 2019. "'MissionRacer': How Amazon Turned the Tedium of Warehouse Work Into a Game." *The Washington Post*.

- Blok, Vincent. 2019a. "From Participation to Interruption: Toward an Ethics of Stakeholder Engagement, Participation and Partnership in CSR and Responsible Innovation." In *Handbook of Responsible Innovation: A Global Resource (Forthcoming)*, edited by R. von Schomberg, and J. Hankins, 243–258. Northampton: Edward Elgar.
- Blok, Vincent. 2019b. "Innovation as *Ethos*. Moving Beyond CSR and Practical Wisdom in Innovation Ethics." In *Handbook of Philosophy of Management*, edited by C. Neesham, and S. Segal, 1–14. Cham: Springer. doi.org/10.1007/978-3-319-48352-8_19-1.
- Borking, John, Huib Gardeniers, Henk van Rossum, Joost Meijers, Paul Overbeek, and Paul Verhaar. 1995. *Privacy-Enhancing Technologies: The Path to Anonymity*. The Hague: Registratiekamer. <https://collections.ola.org/mon/10000/184530.pdf>.
- Brown, Tim, and Barry Katz. 2009. *Change by Design: How Design Thinking Transforms Organizations and Inspires Innovation*. New York: Harper Business.
- Buchanan, Richard. 1992. "Wicked Problems in Design Thinking." *Design Issues* 8 (2): 5–21.
- Cafazzo, Joseph A., Mark Casselman, Nathaniel Hamming, Debra K. Katzman, and Mark R. Palmert. 2012. "Design of an MHealth App for the Self-Management of Adolescent Type 1 Diabetes: A Pilot Study." *Journal of Medical Internet Research* 14 (3): e70. doi.org/10.2196/jmir.2058.
- Casilli, Antonio. 2020. "Preparare, Verificare, Imitare: Perché il Lavoro Umano è Necessario Alla Produzione di Intelligenze Artificiali. L'enigma del Valore. Il Digital Labor e la Rivoluzione Tecnologica." In *Atti del Convegno Organizzato da Effimera, 1° Giugno 2019, Milano, Casa Della Cultura*, 25–41. Milano: Effimera.
- Cavoukian, Ann. 2011. "Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices." Information and Privacy Commissioner of Ontario. Issued 2010; Revised January 2011. https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
- Chappin, Emile J. L., Xanna Bijvoet, and Alexander Oei. 2017. "Teaching Sustainability to a Broad Audience Through an Entertainment Game – The Effect of Catan: Oil Springs." *Journal of Cleaner Production* 156: 556–568. doi.org/10.1016/j.jclepro.2017.04.069.
- D'Acquisto, Giuseppe, Josep Domingo-Ferre, Kikiras Panayiotis, Vicenç Torra, Yves-Alexandre de Montjoye, and Athena Bourka. 2015. "Privacy by Design in Big Data: An Overview of Privacy-Enhancing Technologies in the Era of Big Data Analytics." European Union Agency for Network and Information Security (ENISA). Accessed May 20, 2020. <https://www.enisa.europa.eu/publications/big-data-protection>
- D'Acquisto, Giuseppe, and Maurizio Naldi. 2017. *Big Data e Privacy by Design. Anonimizzazione, Pseudonimizzazione, Sicurezza*. Torino: Giappichelli.
- Datagame. 2016. "Examples of Gamification in the Workplace." Datagame, August 19. Accessed May 20, 2020. <http://datagame.io/examples-of-gamification-in-the-workplace/>
- de Andrade, Norberto Nuno Gomes. 2011. "Data Protection, Privacy and Identity: Distinguishing Concepts and Articulating Rights." In *Privacy and Identity*, edited by S. Fischer-Hübner, P. Duquenoy, and M Hansen, 90–107. Berlin, Heidelberg: IFIP International Federation for Information Processing AICT 352.
- Delfanti, Alessandro. 2019. "Machinic Dispossession and Augmented Despotism: Digital Work in an Amazon Warehouse." *New Media & Society*, 23(1): 39–55. doi:1461444819891613.
- Delfanti, Alessandro, and Bronwyn Frey. 2020. "Humanly Extended Automation or the Future of Work Seen Through Amazon Patents." *Science, Technology & Human Values* 0162243920943665: 1–28. doi:0162243920943665.
- Deterding, Sebastian, Dan Dixon, Rilla Khaled, and Lennart Nacke. 2011. "From Game Design Elements to Gamefulness: Defining 'Gamification' Theory Lenses: Deriving Gameplay Design Patterns from Theories." Paper Presented at the 15th International Academic MindTrek Conference: Envisioning Future Media Environments, Tampere, September 28–30.
- Dewey, John. 1916. *Democracy and Education: An Introduction to the Philosophy of Education*. New York: Columbia University Press.

- Dinev, T., H. Xu, J. H. Smith, and P. Hart. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts." *European Journal of Information Systems* 22 (3): 295–316.
- Ferro, Enrico. 2021. "Oggi lo sciopero Amazon, parlano i lavoratori: 'Ecco perché vi chiediamo di non comprare per 24 ore'." *La Repubblica*, https://www.repubblica.it/cronaca/2021/03/22/news/oggi_lo_sciopero_amazon_parlano_i_lavoratori_ecco_perche_vi_chiediamo_di_non_comprare_per_24_ore_-293266466/.
- Goodstein, Jerry, and Andrew Wicks. 2007. "Corporate and Stakeholder Responsibility: Making Business Ethics a Two-Way Conversation." *Business Ethics Quarterly* 17 (3): 375–339.
- Griffiths, Mark D., and Meredith Alex. 2009. "Videogame Addiction and its Treatment." *Journal of Contemporary Psychotherapy* 39: 247–253.
- Grinbaum, Alexei, and Christopher Groves. 2013. "What is "Responsible" about Responsible Innovation? Understanding the Ethical Issues." In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, edited by Richard Owen, John R. Bessant, and Maggy Heintz, 119–142. London, Hoboken (USA): Wiley.
- Gross, Ralph, and Alessandro Acquisti. 2005. "Information Revelation and Privacy in Online Social Networks (The Facebook Case)." Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES), 71–80. Alexandria VA USA. <https://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf>
- Groves, Christopher. 2011. "Public Engagement and Nanotechnology in the UK: Restoring Trust or Building Robustness?" *Science and Public Policy* 38 (10): 783–793.
- Hense, Jan, Markus Klevers, Michael Sailer, Tim Horenburg, Heinz, Willibald Günthner. 2014. "Using Gamification to Enhance Staff Motivation in Logistics." In *Frontiers in Gaming Simulation. ISAGA 2013. Lecture Notes in Computer Science*, edited by Sebastien A. Meijer, Riitta Smeds, vol. 8264, 206–213. Cham.: Springer. doi.org/10.1007/978-3-319-04954-0_24.
- Herzig, Philipp, Michael Ameling, and Alexander Schill. 2012. "A Generic Platform for Enterprise Gamification." In *2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture*, edited by M. Ali Babar, Carlos. Cuesta, Juha. Savolainen, Tomi Männistö, 219–223. Helsinki: IEEE. doi.org/10.1109/WICSA-ECSA.2012.33.
- Hildebrandt, Mirelle. 2006. "Privacy and Identity." In *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth, 61–104. Antwerp/Oxford: Intersentia.
- Hoepman, Jaap-Henk, et al. 2014. "Privacy Design Strategies." In *SEC 2014, FIP International Federation for Information Processing AICT 428*, edited by N. Cuppens-Boulahia, 446–459. Berlin, Heidelberg: Springer.
- Huizinga, Johan. 1998. *Homo Ludens*. London: Taylor & Francis [orig.in Dutch 1938].
- International Labour Organisation (ILO). 2021. *World Employment and Social Outlook. The Role of Digital Labour Platforms in Transforming the World of Work (Flagship Report)*. Geneva: International Labour Office. [wcms_771749.pdf](https://www.ilo.org/wcmsp5/groups/public/-/dms/-/wcms_771749.pdf) (ilo.org).
- Jones, John Chris. 1992. *Design Methods: Seeds of Human Futures*. New York: John Wiley & Sons.
- Kalloniatis, Christos. 2017. "Incorporating Privacy in the Design of Cloud-Based Systems: A Conceptual Meta-Model." *Information & Computer Security* 25 (5): 614–633. doi.org/10.1108/ICS-06-2016-0044.
- Kalloniatis, Christos, Evangelia Kavakli, and Stefanos Gritzalis. 2007. "Using Privacy Process Patterns for Incorporating Privacy Requirements into the System Design Process." Second International Conference on Availability, Reliability and Security (ARES '07), 1009–1017. Vienna: IEEE. doi.org/10.1109/ARES.2007.156.
- Kalloniatis, Christos, Evangelia Kavakli, and Stefanos Gritzalis. 2008. "Addressing Privacy Requirements in System Design: The PriS Method." *Requirements Engineering* 13 (3): 241–255. doi.org/10.1007/s00766-008-0067-3.
- Kalloniatis, Christos, Evangelia Kavakli, and Efstathios Kontellis. 2009. "Pris Tool: A Case Tool for Privacy-Oriented Requirements Engineering." Paper Presented at the 4th Mediterranean Conference on Information Systems, Athens, September 25–27.

- Lambrinouidakis, C. 2018. "The General Data Protection Regulation (GDPR) Era: Ten Steps for Compliance of Data Processors and Data Controllers." *International Conference on Trust and Privacy in Digital Business*, 3–8. Cham: Springer.
- Learmonth Sr., Gerard P., David Smith, William H. Sherman, Mark A. White, and Jeffrey Plank. 2011. "A Practical Approach to the Complex Problem of Environmental Sustainability: The UVa Bay Game." *The Innovation Journal: The Public Sector Innovation Journal* 16 (1): art. 4.
- Long, T., E. Inigo, and V. Blok. 2020. "Responsible Management of Innovation in Business." In *Research Handbook of Responsible Management*, edited by O. Laasch, R. Suddaby, E. Freeman, and D. Jamila, 606–623. Cheltenham: Edward Elgar.
- Lubberink, R., V. Blok, J. van Ophem, and O. Omta. 2019. "Responsible Innovation by Social Entrepreneurs: An Exploratory Study of Values Integration in Innovations." *Journal of Responsible Innovation* 6 (2): 179–210.
- Lucassen, G., and S. Jansen. August 2014. "Gamification in Consumer Marketing - Future or Fallacy?" *Procedia - Social and Behavioral Sciences* 148: 194–202. doi: [10.1016/j.sbspro.2014.07.034](https://doi.org/10.1016/j.sbspro.2014.07.034).
- Martín, Yod Samuel and Antonio Kung. 2018. "Methods and Tools for GDPR Compliance Through Privacy and Data Protection Engineering" 2018 IEEE European Symposium on Security and Privacy Workshops (Euro&PW), 108–111. London: IEEE.
- Mavroeidi, Aikaterini-Georgia, Angeliki Kitsiou, and Christos Kalloniatis. 2019. "The Interrelation of Game Elements and Privacy Requirements for the Design of a System: A Metamodel." In *Trust, Privacy and Security in Digital Business*, edited by Stefanos Gritzalis, Edgar R. Weippl, Sokratis K. Katsikas, Gabriele Anderst-Kotsis, A. Min Tjoa, and Ismail Khalil, 110–125. Cham: Springer. doi.org/10.1007/978-3-030-27813-7_8.
- Mavroeidi, Aikaterini-Georgia, Angeliki Kitsiou, and Christos Kalloniatis. 2020. "The Role of Gamification in Privacy Protection and User Engagement." In *Security and Privacy from a Legal, Ethical, and Technical Perspective*, edited by Christos Kalloniatis, 132–166. London: IntechOpen. doi.org/10.5772/intechopen.91159.
- Meadows, Dannis L. 1999. "Learning to be Simple: My Odyssey with Games." *Simulation & Gaming* 30: 342–351. doi: [10.1177/104687819903000310](https://doi.org/10.1177/104687819903000310).
- Mokadam, Nahush A., Richard Lee, Ara A. Vaporciyan, Jennifer D. Walker, Robert J. Cerfolio, Joshua L. Hermsen, Craig J. Baker, et al. 2015. "Gamification in Thoracic Surgical Education: Using Competition to Fuel Performance." *The Journal of Thoracic and Cardiovascular Surgery* 150: 1052–1058.
- Nelson, Harold, and Erik Stolterman. 2012. *The Design Way: Intentional Change in an Unpredictable World*. Cambridge, MA: MIT Press.
- Noh, Daeho. 2020. "The Gamification Framework of Military Flight Simulator for Effective Learning and Training Environment." *Electronic Theses and Dissertations*, STARS, University of Central Florida, 259. <https://stars.library.ucf.edu/etd2020/259>.
- Nordby, Anders, Kristine Øygardslia, Ulrik Sverdrup, and Harald Sverdrup. 2016. "The Art of Gamification; Teaching Sustainability and System Thinking by Pervasive Game Development." *Electronic Journal of e-Learning* 14 (3): 152–168.
- Oprescu, Florin, Christian Jones, and Mary Katsikitis. 2014. "I Play at Work—Ten Principles for Transforming Work Processes through Gamification." *Frontiers in Psychology* 5 (14): 1–5, doi.org/10.3389/fpsyg.2014.00014.
- Owen, Richard. 2014. "Responsible Research and Innovation: Options for Research and Innovation Policy in the EU. European Research and Innovation Area Board (ERIAB), Foreword Visions on the European Research Area (VERA)." Accessed February 20, 2019. http://ec.europa.eu/research/innovation-union/pdf/expert-groups/Responsible_Research_and_Innovation.pdf
- Owen, Richard, Phil Macnaghten, and Jack Stilgoe. 2012. "Responsible Research and Innovation: From Science in Society to Science for Society, with Society." *Science and Public Policy* 39: 751–760.
- Owen, R., P. Macnaghten, J. Stilgoe, M. Gorman, E. Fisher, and D. Guston. 2013. "A Framework for Responsible Innovation." In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, edited by R. Owen, J. Bessant, and M. Heintz, 27–50. London: Wiley.

- Pattakou, Argyri, Christos Kalloniatis, and Stefanos Gritzalis. 2017. "Security and Privacy Requirements Engineering Methods for Traditional and Cloud-Based Systems: A Review." *Cloud COMPUTING 2017: The Eighth International Conference on Cloud Computing, GRIDs, and Virtualization*, 145–151. IARI.
- Pattakou, Argyri, Aikaterini-Georgia Mavroeidi, Vasiliki Diamantopoulou, Christos Kalloniatis, and Stefanos Gritzalis. 2018. "Towards the Design of Usable Privacy by Design Methodologies." In *2018 IEEE 5th International Workshop on Evolving Security & Privacy Requirements Engine*, edited by Kristian Beckers, Shamal Faily, Seok-Won Lee, Nancy Mead, 1–8. Banff: IEEE.
- Perryer, Chris, Nicole Amanda Celestine, Brenda Scott-Ladd, and Catherine Leighton. 2016. "Enhancing Workplace Motivation through Gamification: Transferrable Lessons from Pedagogy." *The International Journal of Management Education* 14 (3): 327–335. doi.org/10.1016/j.ijme.2016.07.001.
- Pustovrh, Toni, Franc Mali, and Simone Arnaldi. 2018. "Are Better Workers also Better Humans? On Pharmacological Cognitive Enhancement in the Workplace and Conflicting Societal Domains." *NanoEthics* 12: 301–313. doi.org/10.1007/s11569-018-0332-y.
- Robinson, Laura, Jeremy Schulz, Hopeton S. Dunn, Antonio A. Casilli, Paola Tubaro, Rod Carveth, Wenhong Chen, et al. 2020. "Digital Inequalities 3.0: Emergent Inequalities in the Information Age." *First Monday*, University of Illinois at Chicago Library, 25 (7). <https://firstmonday.org/ojs/index.php/fm/article/view/10844/9562>
- Robol, M., M. Salnitri, and P. Giorgini. November 2017. "Toward GDPR-Compliant Socio-Technical Systems: Modeling Language and Reasoning Framework." IFIP Working Conference on The Practice of Enterprise Modeling, 236–250. Cham: Springer.
- Rodotà, Stefano. 1995. *Tecnologie e Diritti*. Bologna: Il Mulino.
- Rodotà, Stefano. 2016. "Prefazione (Foreword)." In *Privacy. Filosofia e Politica di un Concetto*, edited by M. Bocchiola, 9–16. Roma: LUISS University Press.
- Roessler, Beate. 2005. *The Value of Privacy*. Cambridge: Polity.
- Romanou, A. 2018. "The Necessity of the Implementation of Privacy by Design in Sectors Where Data Protection Concerns Arise." *Computer Law & Security Review* 34 (1): 99–110.
- Ruggiu, Daniele. 2015. "Anchoring European Governance: Two Versions of Responsible Research and Innovation and EU Fundamental Rights as 'Normative Anchor Points.'" *Nanoethics* 9 (3): 217–235.
- Ruggiu, Daniele. 2018. *Human Rights and Emerging Technologies: Analysis and Perspectives in Europe*. Singapore: Pan Stanford.
- Ruggiu, Daniele. 2019. "Models of Anticipation within the Responsible Research and Innovation Framework: The Two RRI Approaches and the Challenge of Human Rights." *Nanoethics* 13 (1): 53–78.
- Ruhi, Umar. 2015. "Level up Your Strategy: Towards a Descriptive Framework for Meaningful Enterprise Gamification." *Technology Innovation Management Review* 5 (8): 12.
- Sand, Martin. 2018. "The Virtues and Vices of Innovators." *Philosophy of Management* 17: 79–95.
- Schwartz, P. M., and K. N. Peifer. 2017. "Transatlantic Data Privacy Law." *Geo. LJ* 106: 115.
- Sousa, Mariana, Ferreira, Duarte; Pereira, Cátia Santos, Bacelar, Gustavo, Frade, Samuel, Pestana, Olívia, and Ricardo Cruz-Correia. 2018. "OpenEHR based systems and the General Data Protection Regulation (GDPR)". In *Building Continents of Knowledge in Oceans of Data: The Future of Co-Created EHealth*, edited by Adrien Ugon, Daniel Karlsson, Gunnar O. Klein, Anne Moen, 91–95. European Federation for Medical Informatics (EFMI) and IOS Press: Copenhagen, Denmark; Amsterdam, The Netherlands. doi:10.3233/978-1-61499-852-5-91
- Stanculescu, L. C., A. Bozzon, R. J. Sips, and G. J. Houben. 2016, February. "Work and Play: An Experiment in Enterprise Gamification." Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, 346–358.
- Tikkinen-Piri, C., A. Rohunen, and J. Markkula. 2018. "EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies." *Computer Law & Security Review* 34 (1): 134–153.

- van den Berg, B., and Ronald E. Leenes. 2013. "Abort, Retry, Fail: Scoping Techno-Regulation and Other Techno-Effects." In *Human Law and Computer Law: Comparative Perspectives*, edited by M. Hildbrandt, and A. M. P. Gaakeer, 67–87. Dordrecht, Heidelberg: Springer.
- von Schomberg, R. 2013. "A Vision of Responsible Research and Innovation." In *Responsible Innovation: Managing the Responsible Emergence of Science and Innovation in Society*, edited by R. Owen, J. Bessant, and M. Heintz, 51–74. London: Wiley.
- Warmelink, Harald, Igor Jonna Koivisto, Igor Mayor, Mikko Vesa, and Juho Hamari. 2020. "Gamification of Production and Logistics Operations: Status Quo and Future Directions." *Journal of Business Research* 106: 331–340.
- Yonemura, Keiichi, Kuniaki Yajima, Ryotaro Komura, Jun Sato, and Yoshihiro Takeichi. 2017. "Practical Security Education on Operational Technology Using Gamification Method." 2017 7th IEEE International Conference on Control System, Computing and Engineering (ICCSC), 284–88. Penang: IEEE. doi.org/10.1109/ICCSC.2017.8284420.