UDC 341.231.14

THE IMAGE OF HUMAN RIGHTS IN E-STATE[1]

M. SUSI[a]

[a]*Tallinn University, 25 Narva Road, Tallinn 10120, Estonia*

The article applies the non-coherence theory of digital human rights to e-statehood and identifies five caveats. The emerging image is characterized by the absence of human rights rhetoric from e-state goals and strategy, absence of conclusive justification of e-state success in social context, relatively lower protection of human rights through e-state solutions in comparison with solutions in the private digital domain, dichotomy of the meaning of privacy in the digital domain, and the theoretical threat of e-state transforming into a police-state. The article argues that since human rights are not generic to e-state, their inclusion into the rhetoric about e-state is the result of public pressure. The author proposes the thesis about negative correlation between the e-state and human rights: the expansion of e-state solutions in a given society leads to decrease in fundamental rights protection.

Keywords: human rights and e-state; non-coherence theory of digital human rights; caveats of human rights; e-state narratives.

ПРЕДСТАВЛЕНИЕ О ПРАВАХ ЧЕЛОВЕКА В ЦИФРОВОМ ГОСУДАРСТВЕ

М. СУСИ[1)]

[1)]*Таллинский университет, Нарвское шоссе, 25, 10120, г. Таллин, Эстония*

Применяется теория несогласованности цифровых прав человека с электронным государственным устройством и определены пять предостережений в этой области. Возникающий образ характеризуется отсутствием прав человека в целях и стратегии цифрового государства, неубедительным обоснованием успеха последнего в социальном контексте, относительно более слабой защитой прав человека посредством решений цифрового государства по сравнению с решениями в частном цифровом домене, дихотомией значения понятия "частная жизнь" в цифровом домене, теоретической угрозой преобразования цифрового государства в государство полицейское. Утверждается, что, поскольку права человека не являются общими для цифрового государства, их включение в обсуждение данного вопроса является результатом общественного давления. Автор выдвигает тезис о негативной корреляции между правами человека и государством: экспансия технологий цифрового государства в обществе приводит к снижению уровня защиты фундаментальных прав.

Ключевые слова: права человека и цифровое государство; теория несогласованности цифровых прав человека; предостережения о правах человека; описания цифрового государства.

[1]Preparation of the article is organized by Raoul Wallenberg Institute of Human Rights and Humanitarian Law in the context of academic cooperation with the Belarusian State University and other Belarusian universities. This academic cooperation has been supported by the Government of Sweden represented by the Swedish International Development Cooperation Agency (Sida). Opinion of the authors expressed in this article may not coincide with the viewpoint of the Institute or Sida.

Образец цитирования:
Суси М. Представление о правах человека в цифровом государстве. *Журнал Белорусского государственного университета. Международные отношения*. 2020;1: 62–68 (на англ.).

For citation:
Susi M. The image of human rights in e-state. *Journal of the Belarusian State University. International Relations*. 2020; 1:62–68.

Автор:
Март Суси – доктор юридических наук; профессор.

Author:
Mart Susi, doctor of science (law); professor.
mart.susi@tlu.ee

Background of the article

Within a relatively short time period in the autumn of 2019 I was invited to speak about the Estonian "achievements" related to e-statehood in Brasilia (Brazil), and Minsk (Belarus). Despite the difference in the composition of audiences – primarily government officials in the first occasions and students in the second, my assumption regarding their expectations was one and the same. The audiences expected an uncritical presentation about Estonia's practical achievements in fostering the image of a technology-oriented society, where the population at large is gladly accepting proposed e-state solutions and lining behind the government. Preparation to these presentations led me to formulate caveats on human rights in e-state. Discussions with the audiences convinced that the magnitude of e-state uncritical narrative needs balancing from the side of human rights academic viewpoint.

Image and theoretical framework

The image. The image of human rights in the context of e-state suggests obscurity and distrust, both rooted in perception of human rights as practice. The obscurity aspect of this image is related to knowledge development and in common language is usually expressed as "the people not understanding how the e-state works". To give a few examples, this aspect has led to the rejection of e-elections, an application of e-statehood capable of affecting the whole society, by the German Constitutional Court, where the court stressed the need for transparency in the electoral process without specialist technical knowledge[2]. M. Solvak and K. Vassil identified in a study of how the Estonian population has accepted the instrument of e-elections as the main challenge the replacement of the "simple trust" towards the public power with better understanding how the systems work and human rights are safeguarded [1]. The epistemic nature of the obscurity aspect of this image prevents the objection to the possibility of safeguarding human rights in e-statehood from becoming absolute. Figuratively speaking, if the principle objection to human rights protection in e-statehood is because of the scarcity of knowledge (like a fog covering some object of interest), then in ideal conditions of knowledge transfer this objection is easily rejected. Because there are no such ideal conditions, the obscurity aspect of this image may constitute a *sine qua non,* ongoing condition of human rights role and position in the sphere of e-statehood or public e-services.

This is because of two justifiable narratives. The first says that technological developments are always a step ahead of conceptualization in social sciences. The second reveals the condition of dichotomy between IT-developers and human rights scholars and activists – that it, IT-developers do not understand human rights potential infringement argument, and the human rights community does not understand what exactly are the IT-solutions capable of doing. In the other words, human rights scholars and activists do not comprehend the full magnitude of how deep and into what details e-state developments can intrude from human rights perspective. Mireille Hildebrandt is pursuing a EC funded advanced research grant to team lawyers and computer scientist with the goal of cross-translation of narratives[3] – this is just an example of the importance of bridging the two communities.

The second aspect of this image is distrust. It originates from blockchain technology and visible or invisible surveillance and analytical capabilities achievable through modern technical solutions. The common argument warns against the possible abuse by the government or public entities from the ground of private information which individuals have been compelled to surrender through various e-state solutions. The objection to trade-off, that is, to obtaining the benefit of living in a modern society claims, that the cost of yielding private and family data is not too high. This objection in principle can be rejected by legal and non-legal arguments.

The legal argument is related to checks and balances and remedies in positive law, that is, whether e-state solutions include sufficient legal mechanisms to minimize the concern that private data obtained is used un-purposefully[4]. Thus, according to the legal argument, it may be possible to set up a system of positive law, including effective remedies, which secures to human rights in the context of e-state solutions comparable protection with the protection against the arbitrary interference by the state in offline situations.

The non-legal argument is about trust towards the public power. In the other words, in an ideal world the process and results of yielding private information to the democratically established government is subject to constitutional restraints, the government enjoys the trust of the civil society and abuses of information surrendered can be occasional, but not systemic.

---

[2]German Constitutional Court judgment of 25 March 2009 in cases BvC 3/07 and BvC 4/07.

[3]See: About COHUBICOL [Electronic resource]. URL: www.cohubicol.com/about (date of access: 23.04.2020).

[4]Some short references may be in order. See: European Court of Human Rights jurisprudence about the matters of big data, for example Big Brother Watch et al v. The United Kingdom of 13 September 2018 No. 58170/13 or the annual reports of the European data protection supervisor, assessing how efficiently the legislation for privacy protection is realized.

The image of human rights protection in the e-state context leads at the first and non-holistic glance to a development exercise. The goal of such exercise is to move ever closer to conditions of perfect knowledge transfer and perfect trust towards the government. The further fully this goal is realized, the more this image turns immune to objections arguing incompatibility of e-state practical solutions and principles with human rights. In further glance and when placing this development exercise into theoretical framework one easily notices its roots in practice-dependency as opposed to human rights as a normative idea[5]. This approach runs counter the proposition of human rights universality and idealism. The practice-dependent aspect is not sufficient to conclude principle compatibility or incompatibility of e-state with human rights promise.

Non-coherence theory of digital human rights. Elsewhere I have proposed the non-coherence theory of digital human rights, which is paradigmatically different from the practice-dependency-independence framework [2]. The digital dimension of human rights can be described via a novel principle that I term the variance principle, which says that this dimension is characterised by a consistent condition of unpredictability and lack of clarity on whether human rights norms, their realisation, related obligations, and remedies against violations as established in the offline world continue to exist online undistorted or, if distorted, what are the degree and consequences of such distortion, or whether they are replaced by online-specific elements. The variance principle claims that ontic and epistemic aspects of human rights from the offline domain may be at variance with these aspects in the online sphere. It is perhaps more accurate to state that offline rules and principles may apply sporadically, but there exists no predictability about the circumstances under which they apply and exactly how. In some instances, they may apply, such as in relation to some concrete online service providers, or in some countries, or regarding some specific rights – and in other instances they may not. See for example similar propositions. S. Schaumburg-Müller writes: "I am not arguing that life online and offline is always completely the same and ought to be regulated in precisely the same manner in all details. What I am arguing is that they are not fundamentally different either" [3]. Or J. Kulesza writes: "Does the Internet's transboundary nature, scale, speed of communication, automation, interconnectivity and invisibility change the way in which we view and protect fundamental rights (privacy, data protection, non-discrimination, due process, presumption of innocence and free speech)? Are human rights online exactly the same as offline or are they modified by the Internet-specific circumstances, possibly impacting their very core?" [4]. The variance principle leads to the non-coherence theory of digital human rights, which claims that human rights law and its application online is characterised by a decrease in transparency, legal certainty and foreseeability. An extreme decrease in these principles means that the online sphere of human rights is characterised by non-transparency instead of transparency, legal uncertainty instead of certainty, non-foreseeability instead of foreseeability and secrecy instead of accessibility. Human rights exist online in a non-coherent system characterised by the fragmentation of human rights normative sources and interpretation through discursive practice, a multitude of actors with changing roles, novel compliance mechanisms or their overall absence, and the systemic dependence on the capabilities of online stakeholders for the protection of human rights, and the systemic susceptibility to utilitarian considerations which are non-resilient to time; that is, considerations which may change swiftly in time at will, like the goals related to the protection of national security or economic interests.

Five caveats

Application of the non-coherence theory of digital human rights leads to the formulation of five caveats.

The first caveat. The first is related to almost complete absence of human rights rhetoric from e-state goals' and strategic commitments. This observation is subjectively cognitive and is based on reading Estonia's strategy documents, observing administrative practices and political rhetoric when Estonia's success story as an e-governed state is presented either domestically or internationally[6].Comparative analysis to justify or reject this observation in principle, and assess its scope and variances may be in order for

[5] For comprehensive discussion about the matter of practice-dependency and practice-independency of human rights, see: *Coutinho L. P.* The practice-dependency of human rights // *La Torre M., Niglia L., Susi M.* (eds). The quest for rights. Ideal and normative dimensions. Cheltenham : Edward Elgar Publishing, 2019. P. 49–64.

[6] Some examples may be in order from Estonia's national strategy documents. Estonia's information society development plan 2020 (in the Estonian language accessible via: https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf) is a strategy document in 45 pages emphasizing that information technology is a crucial tool to raise competitiveness of any economic or social sphere. This document does not contain a single reference to human rights. Strategy "Estonia 2035" is a long-term development strategy to enhance the well-being of the population in the conditions of modern society. The strategy is on 22 pages and contains no reference to human rights.

future purposes. The author's hypothesis claims that the countries which rely on higher amount of e-solutions for the purpose of public administration resort primarily on rhetorical arguments when the issue of safeguarding human rights in through these solutions is raised. This safeguarding is theoretical and illusory. The countries which have quickly and on large scale resorted to e-state solutions demonstrate at a relatively lower degree how exactly these solutions are in line with the obligation to protect human rights.

The aspect of absence is addressed through various practical initiatives and advocacy tasks. The concept of smart cities or human rights cities is built partly on the understanding that human rights need to be fostered at the local levels. For example, L. van Zoonen has suggested a framework for including people's privacy concerns in research, policy and design of smart cities. The work shows that individual citizens or collective citizen groups are ofteh ignored as partners in the development of smart city technologies or innovations [5]. Others have addressed how smart city environment affects people's privacy [6]. More examples could be given about this approach. The author's observations and discussions with researchers and practitioners in the field reveal endemic absence of human rights goals from e-state strategy and practice. The new concepts of human rights by design and human rights by default, when applied to human rights protection mechanisms in digital vertical relations, are indicative that human rights are engrafted into e-state strategy and solutions, that is, they were not part of the e-state philosophy in the first place.

We are trained to think that human rights are connected to social development [7]. Many examples could be given, well known to readers about human rights, how the interests of vulnerable groups were enhanced because of the human rights argument. One can find examples about business success being related to social responsibility of modern corporations. Contemporary human rights discourse seems to accept the proposition that social development and human rights work in tandem. The non-coherence theory of digital human rights suggests that something must be at variance from this picture from offline dimension when reflected into online dimension. I claim that this variance concerns the transformation of the development and tandem argument. In offline world social and perhaps economic development is enhanced or accelerated when taking into account human rights component. In the online world's e-state development, to the contrary, human rights transform from enhancing factor into impediment. Instead of pushing forward with more and new e-state solutions and expanding the e-statehood into new public administration areas, the developers now need to add an element which is not functionally indispensable. Another way to formulate the first caveat is to say, that human rights factor has not yet been integrated into e-state to the extent that it becomes a functional part of the e-state organism. There is no specific vulnerable group who would gain some competitive advantage if pressure upon e-state design would be channelled into e-state solutions taking into account human rights concerns. This is because of the notion of internet vulnerability – we are all vulnerable in front of the internet, this is the notion of collective vulnerability.

The problem originating from this caveat is the strong possibility that, when making further choices about the development of e-state principles and practical solutions, regard towards human rights simply is not a relevant criterion for assessing the justifiability of proposed measures.

The second caveat. The second caveat is related to the absence of conclusive justification about e-state success in social context. It claims that there exists little or no evidence to comprehensively assess the benefits or failure of the e-state project. This can be a continuous condition, at least as long as data emerges to either support or reject the social impact of the e-state project. While the e-state doctrine remains subject to scientific and practical contestations, I will explore whether any relationship exists between happiness and high development of e-state, that is, whether there is some causal relationship between happiness and (or) unhappiness and e-state development in a given country.

The 2019 World happiness report refrains from presenting correlational conclusions between unhappiness and the time spent on digital media, yet it refers to studies that people who limit their time on social media improve their well-being [8]. In short, the report concludes that adolescents who spend more time on electronic devices are less happy, and adolescents who spend more time on most other activities are happier. The 2020 World happiness report explores why people in the Nordic countries seem to be happier than in other countries [9]. Among other observations it refers to a cross-sectional study over 2005–2012 which links improvements in government quality to improvements in well-being. When government quality is divided into democratic and delivery quality, it is the latter which is more strongly related to citizen happiness. These short brushstrokes, while not establishing that more e-state means less happiness, do not establish the contrary either. Yet it remains a question why Estonia as the "most advanced digital society in the world"[7] is ranked only at the 51st place in the 2020 World happiness report. When to view usage of e-state solutions as part of individual digital habits, and comprehend that more digital time usage means less happiness, then digital

[7] A rhetorical statement often used in reference to Estonia's digitalization and e-governance, see for example: We can built a digital society and we can show you how [Electronic resource]. URL: https://e-estonia.com/ (date of access: 23.04.2020).

public services can be viewed as part of the more general behaviour from the individual's perspective. If the former is correct, then more e-state means less happiness.

Another aspect of e-governance which seems worrying to the human rights and IT scholars is the matter of algorithmic prisons – algorithmic "gatekeepers" influence access to various social services and may lead to insurmountable barriers on behalf of the state power [10]. When in face-to-face situations administrative misunderstandings or issues often can be resolved, there is nobody to talk to in many e-state solutions. This second caveat means that the economic or rhetorical "success" of e-statehood easily can overshadow reliable data how e-state affects people's daily lives and well-being.

The third caveat. The third caveat claims that in the digital sphere fundamental rights protection is more comprehensively expected and realized under horizontal than under traditional vertical governance model. The non-coherence theory posits that several core fundamental rights principles change once transposed from the offline domain into the online domain. For justifying or rejecting the third caveat our interest turns to the question, whether there are any significant differences between public and private digital domains vis-à-vis human rights meaning and mechanisms for protection? This question can be explored from the normative perspective, through practice and the capabilities approach.

From the normative side, one notices the growth of soft law instruments calling upon the private internet service providers to respect fundamental rights[8]. Private entities themselves are developing and publishing *modus operandi,* or original terms of service[9].The terms of service of the public sector, a contrario, originate from the off-line environment and appear transposed for providing in the online domain the "same services" as in the offline realm. The variance therefore lies in the origin of the operation models for protecting fundamental rights in the digital domain: the private online service providers rely on original design, whereas the public service providers, e.g. the e-state uses a model which is necessary to manage the offline public domain. Despite contestations against the foreseeability of the terms of service used by the online service providers [11], the fact remains that generically they are meant for the digital environment and thereby strengthen the online service providers per se, whereas the goal of the e-state is not to strengthen e-state applications, but concrete real-world political and power-oriented processes.

The main epistemic question related to the practice of online private companies' and e-state applications is what exactly these two realms are set to accomplish. I see here a wide discrepancy. The private online portals have their whole business model focusing on increasing the economic efficiency of digital solutions, whereas the e-state solutions have the clear target to make public administration more effective, including in the economic aspect. The difference in goals leads to difference in expectations. The private online domain's goal is focusing on accomplishments in the same domain, whereas the public online domain's goal is focusing on accomplishments in the offline domain. I claim that private online companies and portals are expected to protect fundamental rights at a much higher degree than e-state solutions. The matter of capabilities, that is what exactly are different online solutions capable of doing – is therefore much more relevant for private online dimension than for the public dimension (the e-state). Elsewhere I have shown that although private online enterprises are capable of balancing fundamental rights, the balancing entails high degree of arbitrariness due to the incapability of these portals to attach reasons for the balancing decisions [12]. This is evident from the so-called community standards of major internet companies, as well as from individual notification to portal users, where the decision to block or delete information posted by the user is explained by mere reference to non-compliance with the community standards[10]. E-state on the other hand has no requirement to balance conflicting rights, since the collusions of conflicting rights of individual rights-holders having the same weight is excluded. This is because the e-state is not

[8]At the European level, the primary efforts are undertaken by the Council of Europe and the EU. Various instruments exist at the Council of Europe level, such as the Internet governance strategy 2016–2019, or the Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries. The European Commission has adopted the EU Human rights guidelines on freedom of expression online and offline. At the global level the UN Guiding principles on business and human rights and the "Protect, respect and remedy" framework are pertinent.

[9]In recent years, the main global social media actors have published community standards regarding their anticipated actions towards online content. The focus of these standards is against hate speech and (or) clearly illegal content, but there are also guidelines for when legal content affecting someone's privacy can be removed or blocked. These standards neither refer to the international normative human rights architecture, nor do they address the matter of the sameness of online and offline rights. When YouTube writes in its standards that it "reserves the right to make the final determination of whether a violation of its privacy guidelines has occurred", this reflects the doctrine of law as practice. We may use terms like *lex Facebook, lex Twitter*, etc., which means that the origin of digital human rights law has, strictly speaking, a private character.

[10]Consider the recommendation of the Google Advisory Council, which was set up after the Goolge judgment of the CJEU – Case C-131/12Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (13 May 2014). The council suggested in its report para 19, that Google should not attach reasons to individual decisions of blocking or deletion, but should rather publish statistics.

a place where private individuals and (or) companies can advance their rights claims towards one another, it is the platform for exercising state vertical power. When various private stakeholder groups' fragmentation can be categorized through focus to process-driven (the Global network initiative), substance-oriented (Manila principles) and issue-oriented (Google Advisory Council) initiatives, such fragmentation does not emerge in the e-state context. The matter of capabilities does not emerge for public online domain from the aspect of fundamental rights protection, since the e-state has no specific goals related to the protection of fundamental rights other than the ones originating from the offline domain. The main fundamental rights concern for e-statehood is whether the e-state solutions by themselves have secret doors enabling the arbitrary usage of data, which is a matter concerning the following two caveats. The previous leads me to advance the hypothesis that fundamental rights are non-essential for justifying nor realization of e-state solutions. Another way to formulate the same idea is to suggest that e-state does not need fundamental rights, or even more bluntly – fundamental rights disturb the development of e-state.

The fourth caveat. The fourth caveat is related to the dichotomy of the meaning of privacy in the digital domain, and to the perpetual digital memory. The non-coherence theory is based on the recognition that the meaning of human rights norms changes once transposed into the digital domain. The following can be said about the change of the meaning of privacy through digital transposition. The doctrine of privacy fatalism is advanced as a persistent contemporary phenomenon to characterize the distortion of the traditional meaning of privacy online [13–16]. Privacy online has been declared "dead" or "dying" [17], or as the founder of Facebook Mark Zuckerberg says, "privacy is no longer a social norm" [18]. The concerns related to intrusions into privacy by contemporary media, traced to the seminal article by S. D. Warren and L. D. Brandeis introducing the modern concept of privacy (S. D. Warren and L. D. Brandeis [19] for example they lamented and critiqued "the press" which was "overstepping in every direction" beyond common decency and engaging in "vicious" and "unseemly" gossip [20]), have possibly reached an extreme in modern internet-driven technology. It is suggested that the internet has given birth to modern privacy rights, as proposed by several scholars focusing on new technology and associated data practices and threats and challenges to privacy, particularly the development of new computing and data-based technologies [21–24]. The result of this process is that defining and conceptualizing privacy has become an increasingly complex and complicated task [25], which has led to the notion of privacy being divided up and segmented into numerous categories; for example, physical or spatial, decisional, and informational privacy [26]. It has been argued that today nobody appears "to have any very clear idea what privacy is" [27]. The difficulties associated with defining privacy online may have the "chilling effect" of deterring people from exercising their rights and freedoms on the internet [28]. These brushstrokes have to suffice here when painting privacy in the digital domain. Even superficial glance upon the painting notices that this non-coherence between the digital or non-digital domains concerns primarily private online aspect. For e-state the meaning of privacy has not changed at all, or it has changed considerably to a smaller degree, since e-state is mainly concerned with citizens and their privacy phenomenon in the offline realm. Therefore, this fourth caveat leads to the conclusion that the notion of privacy is considerably more complex and many-faceted in private digital domain in comparison with the public digital domain, including e-state.

Private online digital domain is influenced by time and forgetting, whereas the e-state is not and Blockchain never forgets. There is no corresponding entitlement in the public sphere to the right to be forgotten which obligates private online search engines [29] under certain conditions to block access to information which is not relevant for the public. A well-known statement – which is part of popular and scientific folklore – that the Internet knows you better than you yourself can be proven both for private online sphere and for blockchain technology. Only when the private internet companies may be compelled to forget, the blockchain by design is unable to yield to this command.

Against this background we can put forward the caveat about dichotomy in the meaning of privacy in the digital domain. This dichotomy may also exist regarding other human rights norms.

The fifth caveat. Fifth and finally, there is a threat – even if it remains primarily theoretical, of e-state transforming into a police-state. The threat is because blochchain and internet generate many tools which enable such transformation, remaining unnoticed and disguised under the veil of economic and technological efficiency. Such transformation would be accompanied by the rhetoric of trading protection of privacy for increased international and national security[11]. It is sufficient to claim under this fifth caveat that with the expansion of e-state the possibility of police-statehood measures increases. These measures may not become implemented simultaneously. Much more could be written about this threat, but it has to suffice.

[11]For discussion about this matter, see: *Waldron J.* Security and liberty: the image of balance // Journ. Political Philos. 2003. No. 11. P. 191.

Conclusion

The five caveats in conjunction lead me to formulate a thesis about negative correlation between e-statehood and fundamental rights. The spread of e-state usage to more and more public administration areas and by more and more public offices invigorates the development aspect without the need to consider how the new developments coincide with human rights related obligations. The stronger the e-state, the more the human rights factor is withering. Slower development and spread of e-state solutions may signal contestations related to the human rights factor. This thesis will have to be examined in more depth and detail in future writings.

References

1. Solvak M, Vassil K. *E-voting in Estonia: technological diffusion and other developments over ten years (2005–2015)*. Tartu: University of Tartu; 2016. 224 p.

2. Susi M. Human rights in the digital domain: the idea of non-coherence theory. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 3–13.

3. Schaumberg-Müller S. Liability regimes for online human rights violations. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 103– 117.

4. Kulesza J. Multistakeholderism – meaning and implications. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 117– 132.

5. Zoonen van L. Privacy concerns in smart cities. *Government Information Quarterly*. 2016;33(3):472–480.

6. Eckhoff D, Wagner I. Privacy in the smart city – applications, technologies, challenges, and solutions. *IEEE Communications Surveys & Tutorials*. 2018;20(1):489-516. DOI: 10.1109/COMST.2017.2748998.

7. Alston P. Ships passing in the night: the current state of the human rights and development debate seen through the lens of the millennium development goals. *Human Rights Quarterly*. 205;27(3):755–829.

8. Twenge J M. The sad state of happiness in the United States and the role of digital media [Internet; cited 2020 April 23]. Available from: https://worldhappiness.report/ed/2019/the-sad-state-of-happiness-in-the-united-states-and-the-role-of-digital-media/.

9. Martela F, Greve B, Rothstein B, Saari J. The Nordic exceptionalism: what explains why the Nordic countries are constantly among the happiest in the world [Internet; cited 2020 April 23]. Available from: https://worldhappiness.report/ed/2020/the-nordic-exceptionalism-what-explains-why-the-nordic-countries-are-constantly-among-the-happiest-in-the-world/#fnref28.

10. Liu HY. The digital disruption of human rights foundations. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 75–87.

11. Wischmeyer T. The role and practices of online stakeholders. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 148–163.

12. Susi M. Balancing fundamental rights on the Internet – the proportionality paradigm and private online capabilities. In: Torre La M, Susi M, Niglia L, editors. *The quest for rights: ideal and normative dimensions of law*. Cheltenham: Edward Elgar Publishing; 2019. p. 173–194.

13. Mims C. Privacy is dead. Here's what comes next. *Wall Street Journal*. 2018 May 6.

14. Tan A. Privacy is dead. *The Business Times*. 2018 June 9.

15. Bonnell K. Privacy is dead and we all helped kill it. *Ottawa Citizen*. 2018 April 2.

16. Kerry CF. Why protecting privacy is a losing game today – and how to change the game [Internet; cited 2020 April 19]. Available from: https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

17. Richards N. Four myths of privacy. In: Sarat A, editor. *A world without privacy: what the law can and should do*. Cambridge: Cambridge University Press; 2015.

18. Johnson B. Privacy no longer a social norm, Facebook founder says. *The Guardian*. 2010 January 11.

19. Warren SD, Brandeis LD. The right to privacy. *Harvard Law Review*. 1890;4(5):193–220.

20. Glancy DJ. Invention of the right to privacy. *Arizona Law Review*. 1971;21(1):1–40.

21. Rosenberg J. *The death of privacy*. New York: Random House; 1969. 236 p.

22. Regan PM. *Legislative privacy: technology, social values, and public policy*. Chapel Hill: University of North Carolina Press; 1995. 336 p.

23. Froomkin M. The death of privacy? *Stanford Law Review*. 2000;52:1461–1543.

24. Garfinkel S. *Database nation: the death of privacy*. Sebastopol: O'Reilly Media; 2000. 336p.

25. Lin E. Prioritizing privacy: a constitutional response to the Internet. *Berkeley Technology Law Journal*. 2002;17(3): 1085–1154.

26. Kang J. Information privacy in cyberspace transactions. *Stanford Law Review.* 1998;50:1193–1294.

27. Thomas JJ. The right to privacy. In: Schloeman FD, editor. *Philosophical dimensions of privacy: an anthology*. Cambridge: Cambridge University Press; 1984.

28. Penney JW. Chilling effects: online surveillance and Wikipedia use. *Berkeley Technology Law Journal*. 2016;31(1): 117–182.

29. Pagallo U, Durante M. Human rights and the right to be forgotten. In: Susi M, editor. *Human rights, digital society and the law: a research companion*. London: Routledge Publishing; 2019. p. 197–209.

Received by editorial board 28.04.2020.