

Ryszard Piotrowski
Warsaw University

NEW TECHNOLOGIES OR NEW HUMAN RIGHTS: THE RIGHT TO A GOVERNMENT BY HUMANS AND THE RIGHT TO ONE'S OWN THOUGHTS?*

I. THE RIGHT TO A GOVERNMENT BY HUMANS AS A RESPONSE TO THE THREATS THAT NEW TECHNOLOGY PRESENTS TO DEMOCRACY

The rapid development of information and communication technology (ICT) has made it imperative that new human rights be spelled out, to cope with an array of expected threats associated with this process.

With artificial intelligence (AI) being increasingly put to practical uses¹, the prospect arises of Man's becoming more and more AI-dependant in multiple walks of life. This necessitates that a constitutional and international dimension be imparted to a right that stipulates that key state-level decisions impacting human condition, life and freedom must be made by humans, not automated systems or other AI contraptions. But if artificial intelligence were to make decisions, then it should be properly equipped with value-based criteria.

The not inconceivable possibility of humans' being replaced by AI in government and judiciary calls for a re-examination of the very concept of what is referred to as the democratic system. While it seems fair to acknowledge that a democracy may sometimes allow for indispensable restrictions on human rights (with minority rights respected), it must be emphatically demanded that such restrictions may only be imposed by humans exercising legislative, executive or judicial powers – not by algorithms, computer software and applicable AI forms.

Just as with the erosion of the rights to privacy and to informational identity, a creeping process plays out where systems outside of people's control gradually take control of people themselves. Automatic devices and algorithm-based

* Paper presented to The Xth World Congress of International Association of Constitutional Law (2018 Seoul) Organizer's Workshop on "Futuristic Constitutionalism and Sustainability".

¹ Cf. E. Brynjolfsson, A. McAfee, *The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York 2014, pp. 58ff.

software are becoming increasingly autonomous, assuming characteristics of what is referred to as artificial intelligence².

The new threats accompanying the development of new technology provide arguments for enacting new rights, such as the right to be forgotten which is introduced in the data protection regulation. Thus the law of the European Union has enacted a right that may be regarded as a *sui generis* prefiguration of the right proposed in the present article, namely the right to be governed by people, and not by automata, algorithms, neural networks, or such devices (being developed now and in future) that are referred to as artificial intelligence.

In Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealed with effect from 25 May 2018, the right was established to freedom from being governed by automated data processing. In its Article 15, the Directive reads:

“Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.”.

In Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Article 22.1 reads:

“The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her”.

However, this paragraph “shall not apply if the decision: a) is necessary for entering into, or a performance of, a contract between the data subject and a data controller; b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests; or c) is based on the data subject’s explicit consent”. Regulation ensures in its Article 22 paragraph 3: in the cases referred to in points a) and c) “the data controller shall implement suitable measures to safeguard the data subject’s rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her points of view and to contest the decision”.

According to the Report of the Committee on Legal Affairs (European Parliament)³ the developments in robotics and artificial intelligence can and should be designed in such a way that they preserve the dignity, autonomy and self-determi-

² Cf. N. Bostrom, *Superintelligence. Paths, Dangers, Strategies*, Oxford 2014, pp. 23ff.

³ Cf. European Parliament. Committee on Legal Affairs: *Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103 (INL)), p. 5.

nation of the individual; the possibility of human control and verification need to be built into the process of automated and algorithmic decision-making.

In everyday life, in step with the expansion of automated services, automated stock exchange transactions and the emergence of the internet of things, the condition of man has been increasingly impacted by non-human entities⁴. And the decisions taken by software has been increasingly legitimised by humans. The growing dehumanisation of the way human requirements are being met is very likely as unstoppable as the erosion of privacy.

This is all the more reason to emphasise the importance of the maxim *habeas potestatem humanam*. The legislative, executive and judicial prerogatives must not be ceded to software or other decision-making programmes, including those referred to as artificial intelligence.

From the principle of the dignity of human person there arises a crucial human right, one that deserves being noticed and promoted – namely the right that decisions impacting the legal and political situation be undertaken by people and not by tools, even the most elaborate ones. Such tools, notwithstanding their high performance levels, will lack human-specific potential, as arising from the ability to empathise and experience emotions, such as joy, suffering or doubting.

The constitutions of democratic states lay down the principles of government by sovereign people, not by sovereign algorithms. Sovereignty is founded on the freedom of choice, which involves dialogue, persuasion and deliberative decision-making. The current forms of artificial intelligence are not capable of a knowledge- and culture-based reasoning, nor can they engage in a dialogue that could persuade them to change opinion and switch to a particular solution. No such tool has yet been developed that would cultivate human-specific spiritual culture. No way has been found yet to produce that what makes us human, that which cannot be counted, measured or weighed. It is highly unlikely for values to be instilled in a machine in a process of learning, remembering how difficult it is to instil them in so many people.

The democratic system is inseparably linked with human agency, not with even the most sophisticated man-made tools. The right to be governed by humans is among the basic human rights. Lack of human control over the tools may well be a harbinger of catastrophe, but it is by no means a feature of the democratic system. Consequently, constitutions should confirm the right to be governed by humans, or in other words the right that the status of an individual – his or her rights, freedoms and obligations – be not defined by software alone.

People use increasingly complex software as their tools, and the refined tools tend to gradually become more and more autonomous, thus posing a potential threat to the dignity of the human person, their rights and freedoms and their life. Killer robots and lethal autonomous weapons will permit armed conflict to be

⁴ Cf. S. Rodota, *Il diritto di avere diritti*, Bari 2012, p. 376.

thought at a scale greater than ever⁵. Obviously, where the effectiveness of human activity can be strengthened – in respect of, for example, medical diagnosis or legal analysis preceding a court ruling – it is reasonable to use the tools that are available. But these tools must not supersede the key human factor in the decision-making process.

Tools, and especially the artificial neural networks, may be biased. Bias may well be inherent in the historical data fed into the neural networks⁶ for the purpose of learning. An uncritical use of such tools may thus produce discriminatory consequences⁷.

Although this may not yet be the case, algorithms can be used in a manner that is immanently risky. The risk is incurred by the use of algorithms to determine people's traits based on facial features or the vocabulary used⁸, and to establish their psychometric characteristics – particularly in finding out who may prove to be a criminal⁹.

If we accept that neural networks are capable of determining a person's proclivity to aggression based on his or her facial features with, for example, 80% certainty¹⁰, then people will be prone to use this information in certain situations, for example at airport security checks. An algorithm that is effective within certain bounds will thus – in certain situations – discriminate against a person based on his or her outward appearance. This glaringly contradicts the constitutional principles and culturally accepted values of democratic nations. As matters stand now, algorithms do not yet make decisions. Decisions are made by people, taking into account the outcome of algorithms. And this is where a real threat is now present. The use of algorithms may restrict human dignity, confining it to mere data points. Right now, algorithms are used to influence voting behaviour so intensely as to warrant the possibility that voters may be left with no say on election results.

While artificial intelligence will certainly embrace a reasoning capability in future, it is not clear whether it will be capable of understanding human

⁵ Cf. S. Gibbs, *Elon Musk leads 116 experts calling for outright ban of killer robots*, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war> (accessed: 30.10.2018).

⁶ Cf. I. Goodfellow, Y. Bengio, A. Courville, *Deep Learning*, Cambridge–London 2016.

⁷ Cf. J. L. Skeem, Ch. Lowenkamp, *Risk, Race, & Recidivism: Predictive Bias and Disparate Impact*, "Criminology" 2016, Vol. 54, issue 4, pp. 680ff; see also: V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York 2017.

⁸ Cf. J. Baugh, *Linguistic Profiling and Discrimination*, (in:) O. García, N. Flores, M. Spotti (eds.), *The Oxford Handbook of Language and Society*, Oxford 2017, pp. 349ff.

⁹ Cf. J. Tashea, *Courts Are Using AI to Sentence Criminals. That Must Stop Now*, <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now> (accessed: 30.10.2018).

¹⁰ Cf. X. Wu, X. Zhang, *Automated Inference on Criminality using Face Images*, <https://arxiv.org/abs/1611.04135v1> (accessed: 30.10.2018).

problems¹¹. It cannot be ruled out that future constitutions will accept something that is as inconceivable today as racial equality was in the past. According to European Parliament Report of 2017 “ultimately there is a possibility that in the long-term, AI could surpass human intellectual capacity”¹².

The importance of the right to be represented, governed and judged in court by humans is highlighted by the prospect of threats that may arise if control of society is taken over by the tools intended to serve its security. It may turn out that – when it comes to defining security – these tools may begin to dangerously play a role that transcends their original remit.

This threat of algorithms’ influencing the will of vacillating voters who are active on social networks is already making itself felt in modern democracies. In step with the development of information and communication technology, independent thinking skills are seen as being on the decline, reflecting an individual’s growing dependence on technology as a tool to facilitate and intermediate in the thought process¹³. *Homo sapiens* is also said to be turning into *homo videns* – a tractable man exposed to media manipulation and increasingly defenceless against TV and online messaging¹⁴.

In the time of Thucydides, democracy was described by Pericles as respecting the differences among individuals and their privacy – and he saw the democratic system as one where citizens do not exercise “a jealous surveillance over each other”¹⁵. Going back in time, we find in Homer the belief that law cannot rule unless created by all those to be governed by it, those whom in today’s parlance we would call autonomous lawmakers, whose opinions are neither subject to control nor to formatting. In Homer’s words, the barbarians “have no assemblies for political discussion, nor laws”¹⁶ – and it is precisely in assemblies that law is made by all members of the community, free in their decisions from fear of being controlled by those capable to exercise control. The less of privacy, the greater the risk that an individual’s position in society and his or her requirements will be ignored, to satisfy the real or only declared interests of the majority, as represented – and possibly influenced – by those holding power in a democracy.

¹¹ Cf. M. Tegmark, *Life 3.0 Being human in the age of Artificial Intelligence*, London 2017, pp. 306ff.

¹² Cf. European Parliament. Committee on Legal Affairs: *Report with recommendations to the Commission on Civil Law Rules on Robotics* (2015/2103 (INL)), p. 5.

¹³ Cf. H. Kissinger, *World Order*, London 2014, pp. 350ff.

¹⁴ Cf. G. Sartori, *Homo videns. Televisione e post-pensiero*, Roma–Bari 1997, pp. 104ff.

¹⁵ Cf. Thucydides, *Wojna peloponeska* (Thucydides, *The History of the Peloponnesian War*), Warszawa 1988, p. 107.

¹⁶ Homer, *Odyssey*, Book IX, lines 112ff.

II. THE DESTRUCTION BY NEW TECHNOLOGY OF THE RIGHT TO PRIVACY AS A THREAT TO THE FOUNDATION OF THE DEMOCRATIC SYSTEM

Information and communication technology (ICT) development poses a threat to the privacy of the individual, which is of paramount consequence for the operation of the democratic system¹⁷. Democracy, understood as a debate to seek truth and collaboration, can only be practiced if its participants are free agents whose identity is respected, meaning that they are empowered to define the limits of access to their thoughts and to information that denotes human existence in the world. Human dignity in a modern information society is defined by a person's ability to control data about themselves.

The right to possess all the information about a given individual – adding up to his or her informational identity – may only be vested in that very person. Taking over control of data that are key to a person's distinctness and separateness paves the way to taking over control of his or her identity, which results in identity's being no longer a determinant of that person's free agency. In this sense, the informational identity of the individual comes as his or her inherent and inalienable feature, coessential with his or her dignity.

The very survival of the democratic system, with its roots in the dignity of the person, requires that the right to privacy and protection of personal data be guaranteed.

In actual practice, though, the right to privacy is among the rights most threatened and most illusory¹⁸. Privacy is valued neither by citizens nor the public authorities. At a time of widespread digitalisation, using new technology is a prerequisite of not only getting skills and jobs but also of participating in culture. With this use, however, often comes uncritical and unreflective abdication of one's own privacy. Incessant use of electronic communication being a must in public and social life, the abandonment of privacy – stimulated by fashions that make new technology solutions highly coveted and sought after – becomes a characteristic feature of an emerging new culture. This new culture, determining an individual's existence in the digital community, is founded on more or less conscious relinquishment of informational autonomy and of the related right of the individual to decide which information about himself or herself he or she is willing to disclose to others, and especially to government and business.

The very *raison d'être* of the state, after all, lies in its protecting the human rights. But as matters stand, the state's ineffectiveness in endorsing privacy, and

¹⁷ Cf. T. Garton Ash, *Free Speech: Ten Principles for a Connected World*, New Haven–London 2016, pp. 283ff.

¹⁸ Cf. B. Schneier, *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, New York–London 2015, pp. 125ff.

its infidelity to this constitutional value, is met in practice with public acquiescence. No-one can be forced to care about privacy in the name of his or her dignity or to fight for a freedom which he or she does not need and does not understand – such attitudes being additionally reinforced by national governments and by the global digital order. The tools used by people not only change the world, they also change the people themselves – thus changing the hierarchy of values, which lasts only as long as people manage to distinguish between freedom and such phenomena as “voluntary servitude” or “instinctive, suicidal ineffectiveness of systems of power”¹⁹.

There can be no public- or private-interest justification for depriving an individual of their informational identity or stripping them of their dignity. The right to informational identity, which is coessential with the dignity of the human person, should thus be viewed as effective not only *vis-à-vis* public authority – as is the case with the rights to privacy and to informational autonomy – but also *vis-à-vis* private parties, much in the same vein as with the right to dignity.

Where all available data about an individual are collected by a single entity and integrated into a cohesive profile – without that individual’s knowledge or will – this means that he or she is deprived of something much more valuable than the right to privacy, which after all is subject to restriction. This more valuable thing is the right to possess and dispose of all the data that reflect and confirm the existence and separateness of the individual.

Governments eagerly take advantage of the ongoing erosion of privacy as a cultural value and they tend to establish databases – even if previously the state could well do without these tools, while posing no imminent threat to constitutional values. Getting hold of integrable databases, governments can set up individualised profiles, without the knowledge or will of those concerned.

In a situation marked by an excessive use of new technology, coupled with a rash and unreflective push towards computerisation, data collection may become a goal in itself, regardless of the real practical needs. This leads to an informational totalitarianism, where that segment of the executive branch of government which is capable of data integration will have access to nearly complete knowledge about everyone²⁰.

The capacity to store in one place the information originating at different nodes of an information network presents previously unknown threats to the right to privacy. Exploiting the connivance of citizens and ineffectiveness of their resistance, governments eagerly take advantage of the new opportunities. Increasingly

¹⁹ Cf. J. Baudrillard, *Le pacte de lucidité ou l’intelligence du mal*, Paris 2004, p. 136.

²⁰ Cf. R. Piotrowski, *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym (Right to informational identity in a democracy)*, (in:) J. Jaskiernia (ed.), *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka, (The impact of international standards on the development of democracy and protection of human rights)*, Vol. 1, Warszawa 2013, pp. 490ff.

dependent on their intelligence services, democratic governments take interest in collecting data and developing related technology – and they are aided in this by the widespread nature of such practices and absence of an effective opposition from citizens.

Where the state or another entity is vested with the right to access all information about a free person, the latter is turned into a kind of digital slave, being owned by parties who – claiming concern for his or her own security, convenience or common good – know about that individual even more than he or she knows themselves.

The modern state shows no intention of protecting the privacy of its own citizens against threats that it creates itself, yielding to a digitalisation mania and gathering as many data as it can. Nor does it undertake any effective attempts to curtail the interference in individuals' informational autonomy from private parties – especially the interference made in connection with the business of supplying surveillance tools and surveillance services. The state is not capable of providing “protection of privacy against the monitoring of various walks of citizens' life, including against the messages sent via telecommunication networks by foreign parties, and especially by foreign states”²¹.

In a situation where an individual's footprints in the worldwide web are all but permanent, and where it is not particularly difficult to take control of the digital trail left at various stages of information exchange, the need emerges for a regulation that – while balancing various arguments for protection of the common good, and technological constraints – would not sacrifice the dignity of the person on the altar of public or private interest.

Democracy, understood along the lines of Karl Popper's approach, as a pathway to knowledge, is coessential to a civic society that consists of empowered individuals without whom no authentic debate is possible and no minority rights are respected. And this empowerment rests on individuals' right to separateness, which includes the right to control information about oneself. Acting more or less consciously, individuals do consent to restrict this right in various degrees, especially while participating in public life. But the right to access all information about a person – representing his or her informational identity – can only be held by that very person. Taking over control of data of importance for a person's separateness is equivalent to taking over control of his or her identity, which then no longer defines that person's agency and empowerment. The informational identity, so understood, comes as an inherent and inalienable feature of an individual, coessential with his or her dignity.

The right to privacy is viewed as a limitation on public authority. But in the contemporary world, the privacy of an individual also faces major threats from the operation of private entities, most notably the global corporations. The con-

²¹ See the memorandum of explanation to the Constitutional Tribunal's ruling K 23/11.

cept of the right to privacy as well as the ensuing constitutional and international-law regulations, however, fail to protect individuals against threats to their informational identity coming from the private parties – just as they fail in relations with state actors.

It now comes as an immanent feature of government in an information society that it interferes with the privacy of the individual, posing a threat to his or her informational autonomy “by demanding such information about the individual as is convenient to public authority, even where it is unnecessary”²². In the opinion of the Polish Constitutional Tribunal, data collection “is a typical modern-time instrument that is eagerly deployed by public authority, serving to reinforce the latter’s position *vis-à-vis* the individual”²³.

A society subjected to total surveillance and control – whether by public authority or private parties – would be the exact opposite of civil society, because it would lose an ability to self-organise independently of the controllers of collected information.

Political change and growth of the internet have combined to enable an informational integration on a previously unimaginable scale, laying the groundwork for economic globalisation, defined as an “integration of national economies into the international economy through trade, direct foreign investment (by corporations and multinationals), short-term capital flows, international flows of workers and humanity generally, and flows of technology”²⁴. These processes, taking place outside the control of governments and publics in constitutional democracies, and only to a limited degree dependent on other states, have considerably weakened both parties. The ability to collect data from various parts of an information network in one place poses privacy threats unknown in the past. Globalisation, reflected today in states’ increasing economic interdependence, comes as a result of the pursuit of profit maximisation – not a concern for human rights, which have no market value. With globalisation imposing economic efficiency as the main goal for public authority, the axiological identity of democratic states comes under threat. The development of new technology, the expansion of globalisation and the practice of treating information as a commodity put individual privacy in jeopardy – to a degree bordering on almost total elimination. The new technological opportunities and cultural changes threaten not only the right to privacy, but also the right to informational identity.

International and national standards have proved ineffective in confrontation with the ascendancy of global surveillance²⁵, privacy policies of companies such

²² See the memorandum of explanation to the Constitutional Tribunal’s ruling K 8/04.

²³ *Ibidem*.

²⁴ On definition of globalisation cf. J. Bhagwati, *In Defense of Globalization*, New York 2004, p. 3.

²⁵ On this subject cf. *European Parliament: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))*.

as Google and Facebook²⁶, the professionalism of data analytics agencies, and the rise of a culture of passively giving up on privacy while using the internet and mobile communication. The dreams of totalitarian rules are coming true. Government can now be privy to any information about all, with almost everyone engaged in digital self-reporting. It would indeed be a stretch to describe as democratic a system that satisfies such governmental needs and that can be used to exert total control, against which this system remains either wholly indifferent or defenceless. It well may be that democracy will vanish unless the erosion of values coessential to human dignity – including the respect for privacy – is reversed.

III. THE RIGHT TO ONE'S OWN THOUGHTS AS A RESPONSE TO TECHNOLOGY-RELATED THREATS TO DEMOCRACY

Globalisation would not be possible without new information technology, similarly as representative democracy would not be possible without printing. These two inventions, though, just as any technology, carry both an opportunity and a threat to human rights. The internet contributes to the erosion and a weakening of state sovereignty, but, just as other information technologies, it may help government to subject individuals to nearly total control. The IT growth is a favourable development because it offers new communication opportunities, helps strengthen civic society and facilitates free public debate that is indispensable for democracy's continued existence. At the same time, however, it prods people into a more or less realised abandonment of their own privacy, and into gradually getting used to a world where participation in social life through data exchange, consumption or production is becoming equivalent to giving up on privacy. This is because one's very existence came to be linked with the surrender of privacy. Almost from conception people are subject to either private or public surveillance of digital marks of their existence, which remain virtually indelible.

Just by participating in the worldwide web and uncritically accepting the information system as the basis for operation of the state and society, we all become dependent on this system's controllers, among them the profit-seeking global corporations that deal with information processing. Governments have no say on who will get the data and how long they will be stored. This is the prerogative

²⁶ In 2007, Facebook's privacy policy contained this passage: "By using Facebook, you are consenting to have your personal data transferred to and processed in the United States (...) This may include sharing information with other companies, lawyers, agents or government agencies". Cf. <http://www.guardian.co.uk/technology/2008/jan/14/facebook> (accessed: 30.10.2018). Cf. also *Facebook's Eroding Privacy Policy: A timeline*, <http://www.eff.org/deeplinks/2010/04/facebook-timeline> (accessed: 30.10.2018).

of corporation owners, who sometimes may allow for information to be shared. Before the internet, a sovereign state would never had given its implicit consent to such access to insights about its citizens. Today, however, without ceding any competences and – as is the case with Poland – under a constitutional regime that requires the public authority to protect citizens' security, the state takes kindly to an arrangement where various data about citizens – including their images – are made available to multiple entities, from whom no security guarantees are demanded other than those offered by those entities themselves.

There emerges a system of total and global individualised control of people, extending into more and more manifestations of a person's existence, and especially his or her presence, beliefs and – in the future, perhaps – also their thoughts. Anyone who exists is qualified for being watched and, as such, becomes a suspect.

Modern democracies are too weak *vis-à-vis* multinational corporations, and they have been all too successful in convincing citizens that security and convenience matter much more than respect for human rights. A dominant culture among democratic societies is one of unreflective satisfaction from the present moment, while the privilege of ruminating on the future is left to individuals who, as a rule, exert no influence on the course of public affairs.

Governments may go on believing that human rights, including the right to privacy, are about relations between government and the individual, that constitutions do not operate horizontally, and that international law, including its privacy-related provisions, binds states only as far as it suits their interests.

The effectiveness of the right to informational identity is contingent on whether or not the concept of horizontal operation of human rights and freedoms is accepted. In accordance with this concept, states cannot afford protection to private-law acts and “cannot absolve themselves from responsibility by delegating their obligations to private bodies or individuals”²⁷.

Democracy has found itself in a technology trap. Stanisław Lem saw such a trap in the “outcome of a widespread deployment of technogenic solutions, which turns the purported benefits of such widespread deployment into an either one- or many-sided catastrophe, one that becomes more and more recognisable and less and less preventable by those powerful decision-makers to whom this catastrophe owes its prolific extent and strong destructive qualities”²⁸.

The culture of abdication of privacy protection may breed consent to the creation and practical use of technologies capable to penetrate an individual

²⁷ See the judgement by the European Court of Human Rights in the case of *Costello-Roberts v. the United Kingdom*, 8 October 1991, A.247-C, par. 27.

²⁸ Por. S. Lem, *Pułapka technologiczna (Technology trap)*, (in:) *Dzieła (Works)*, Vol. XXX, Warszawa 2010, p. 115.

consciousness without his or her consent²⁹. Evidence based on such thought interference should be barred from court proceedings. Everyone's right to intellectual identity and integrity, the right to one's thoughts being free from technological interference, is as essential for the survival of the democratic system as the right to privacy – and it may well prove equally endangered.

The right to personal inviolability, understood as prohibition on its arbitrary breach by government – and reflected in the centuries' old principle of *habeas corpus* – needs to be reinterpreted. Given the potential threat of interference in a person's mind without that person's consent, it is imperative that constitutions and international law proclaim the principle of *habeas mentem*. This very principle, reflecting the need to provide guarantees for human internal freedom, may prove to be the last redoubt of human dignity, threatened as it is by loss of the rights to privacy and to informational identity. Thus, it is the freedom of thought that eventually may prevent the push for profit maximisation and control from becoming the dominant motive behind deployments of new technology, which – if materialising – would deal a painful blow to respect for human dignity.

BIBLIOGRAFIA

- Baudrillard J., *Le pacte de lucidite ou l'intelligence du mal*, Paris 2004
- Baugh J., *Linguistic Profiling and Discrimination*, (in:) O. García, N. Flores, M. Spotti (eds.), *The Oxford Handbook of Language and Society*, Oxford 2017
- Bhagwati J., *In Defense of Globalization*, New York 2004
- Bostrom N., *Superintelligence. Paths, Dangers, Strategies*, Oxford 2014
- Brynolfsson E., McAfee A., *The Second Machine Age. Work, Progress, and Prosperity in a Time of Brilliant Technologies*, New York 2014
- Eubanks V., *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York 2017
- European Parliament. Committee on Legal Affairs: Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))
- European Parliament. Committee on Legal Affairs: Report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103 (INL))
- European Parliament: Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))
- Facebook's Eroding Privacy Policy: A timeline, <http://www.eff.org/deeplinks/2010/04/facebook-timeline> (accessed: 30.10.2018)
- Garton Ash T., *Free Speech: Ten Principles for a Connected World*, New Haven–London 2016

²⁹ Cf. M. B. Hoffman, *Nine Neurolaw Predictions*, "New Criminal Law Review" 2018, Vol. 21, No 2, pp. 212ff.

- Gibbs S., *Elon Musk leads 116 experts calling for outright ban of killer robots*, <https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war> (accessed: 30.10.2018)
- Goodfellow I., Bengio Y., Courville A., *Deep Learning*, Cambridge–London 2016
- Hoffman M. B., *Nine Neurolaw Predictions*, “New Criminal Law Review” 2018, Vol. 21, No 2
- Homer, *Odyssey*, Book IX, lines 112ff
- Kissinger H., *World Order*, London 2014
- Lem S., *Pułapka technologiczna (Technology trap)*, (in:) *Dziela (Works)*, Vol. XXX, Warszawa 2010
- Piotrowski R., *Prawo do tożsamości informacyjnej i jego znaczenie w ustroju demokratycznym (Right to informational identity in a democracy)*, (in:) J. Jaskiernia (ed.), *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka (The impact of international standards on the development of democracy and protection of human rights)*, Vol. 1, Warszawa 2013
- Rodota S., *Il diritto di avere diritti*, Bari 2012
- Sartori G., *Homo videns. Televisione e post-pensiero*, Roma–Bari 1997
- Schneier B., *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*, NewYork–London 2015
- Skeem J. L., Lowenkamp Ch., *Risk, Race, & Recidivism: Predictive Bias and Disparate Impact*, “Criminology” 2016, Vol. 54, issue 4
- Tashea J., *Courts Are Using AI to Sentence Criminals. That Must Stop Now*, <https://www.wired.com/2017/04/courts-using-ai-sentence-criminals-must-stop-now> (accessed: 30.10.2018)
- Tegmark M., *Life 3.0 Being human in the age of Artificial Intelligence*, London 2017
- Tukidydes, *Wojna peloponeska (Thucydides, The History of the Peloponnesian War)*, Warszawa 1988
- Wu X., Zhang X., *Automated Inference on Criminality using Face Images*, <https://arxiv.org/abs/1611.04135v1> (accessed: 30.10.2018)

NEW TECHNOLOGIES OR NEW HUMAN RIGHTS: THE RIGHT TO A GOVERNMENT BY HUMANS AND THE RIGHT TO ONE'S OWN THOUGHTS?

Summary

The rapid development of information and communication technology has made it imperative that new human rights be spelled out, to cope with an array of expected threats associated with this process.

With artificial intelligence being increasingly put to practical uses, the prospect arises of Man's becoming more and more AI-dependant in multiple walks of life. This

necessitates that a constitutional and international dimension be imparted to a right that stipulates that key state-level decisions impacting human condition, life and freedom must be made by humans, not automated systems or other AI contraptions. But if artificial intelligence were to make decisions, then it should be properly equipped with value-based criteria.

The culture of abdication of privacy protection may breed consent to the creation and practical use of technologies capable to penetrate an individual consciousness without his or her consent. Evidence based on such thought interference must be barred from court proceedings. Everyone's right to intellectual identity and integrity, the right to one's thoughts being free from technological interference, is as essential for the survival of the democratic system as the right to privacy – and it may well prove equally endangered.

KEYWORDS

new technologies, human rights, artificial intelligence, democracy, right to privacy, the right to a government by humans, the right to one's own thoughts

SŁOWA KLUCZOWE

nowe technologie, prawa człowieka, sztuczna inteligencja, prawo do prywatności, prawo do rządu sprawowanego przez ludzi, prawo do własnych myśli