Guest Editorial

Sokratis K. Katsikas

Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS),
Norwegian University of Science and Technology,
Postboks 191, Gjøvik N-2802, Norway
Email: sokratis.katsikas@ntnu.no

Vasilios Zorkadis

Hellenic Data Protection Authority,
Kifissias 1-3, Athens 11523, Greece
Email: zorkadis@dpa.gr

Biographical notes: Sokratis K. Katsikas is the Director of the Norwegian Centre for Cybersecurity in Critical Sectors and Professor with the Department of Information Security and Communication Technology at NTNU. In 2019, he has awarded a Doctorate Honoris Causa by the Department of Production and Management Engineering of the Democritus University of Thrace, Greece. He is serving on the editorial board of several scientific journals and he has served on/chaired the technical programme committee of more than 800 international scientific conferences. He chairs the Steering Committee of the ESORICS Conference and he is the Editor-in-Chief of the *International Journal of Information Security*.

Vasilios Zorkadis has been working as the Secretariat's Director of the Hellenic Data Protection Authority since 2004. He received a Diploma in Electrical Engineering from Aristotle University of Thessaloniki, Greece and holds a PhD on Computer Network Security from University of Karlsruhe, Germany. He is author of books on 'Cryptography', and 'Information Theory' and author or co-author of more than 60 journal and conference papers on security and privacy protection. He taught for almost 20 years in Greek universities courses on Information Theory, Information Security, Cryptography, Computer Networks and Digital Communications. He is a founding member and the current president of the "Hellenic Council for the Information Society".

The ever-evolving digital age is becoming more intelligent and the future internet is shaping up. Technologies supporting the digital transformation, such as artificial intelligence, the Internet of Things, blockchain technologies, and robotics are developing at unprecedented rhythms. A new digital environment emerges, promising a lot, but also raising concerns about democracy itself and individual rights and freedoms. The Cambridge Analytica scandal has profoundly influenced public opinion and – as written by many – has changed the world and the way citizens see their digital future. The effects of fake news and targeted political campaigns enabled by data misuse on democratic processes raise serious concerns. There are also fears of affecting the outcome of a democratic election itself. Moreover, the rapid development of technologies supporting the digital transformation, which is largely driven by significant economic

benefits, raises concerns about the impact on privacy and, in general, on individual rights and freedoms. These reflections give rise to the following questions:

- How can we safeguard our democracy against such threats?
- How can we create an intelligent digital world while ensuring individual rights and freedoms?
- Will our future digital world be privacy-friendly and secure to withstand attacks and malicious activities?
- Which ethical principles should govern the evolution of our digital future?
- Will this fast moving and intelligent digital world be trustworthy and embraced by the citizens?

These were the questions and the focus of the 8th occasion of the International Conference on e-Democracy that was held in Athens, the cradle of democracy, on December 12–13, 2019. This special issue contains extended and expanded versions of 11 selected papers that were presented in the conference.

The first four papers in the special issue form a cluster on privacy and data protection. The first one, entitled 'Sensitive data hiding in financial anti-fraud process', by Verykios et al. presents an approach to protect personally identifiable information in compliance with the national and EU data protection framework in a way that still allows interoperability of information systems and applications. The authors propose to adopt privacy-preserving information hiding techniques to facilitate targeted data mining without infringing privacy restrictions, so as to contribute to the strategic modernisation of public authorities and financial organisations.

The second paper, entitled 'Exploring data subjects' knowledge on the rights GDPR guarantees: an exploratory research in Greece', by Sideri et al. investigates the knowledge of a Greek adults group regarding the rights GDPR guarantees and reveals fluctuations in such knowledge related to the information sources on GDPR, data subjects concerns and the socio-demographic characteristics of the participants. The findings highlight the need for data subjects to have more information on GDPR and become fully aware of their rights in order to protect their data.

The third paper, entitled 'Big data analytics in e-government and e-democracy applications: privacy threats, implications and mitigation', by Mavriki and Karyda identifies privacy threats for citizens stemming from the use of big data in e-government and e-democracy applications; analyses the challenges for e-government; and explores the challenges of the privacy threats for e-democracy. The authors argue, among others, that automatic decision-making may lead to discrimination compromising equality, a basic democratic value; that decreased privacy facilitates manipulation, polarisation and disinformation. Additionally, the authors critically examine relevant technical privacy enhancing solutions which may play a significant role in shielding democracy through allowing citizens to freely share, access and discuss information and content that is contrary to political, religious or social views of governments.

The fourth paper, entitled 'Privacy issues in Android applications: the cases of GPS navigators and fitness trackers', by Monogios et al. follows a more technical approach and studies privacy issues in the mobile ecosystem, focusing on two important types of smart applications which process personal data to a large extent: global positioning system (GPS) navigators and fitness tracking applications. For both types of applications,

an indicative list of popular apps is analysed and the underlying personal data processing is identified. The analysis reveals that both GPS navigation apps and fitness trackers have access to several types of users data, while they may allow for personal data leakage towards third parties such as library providers or tracking services without necessarily providing adequate or precise information to the users.

The next two papers address issues related to biased and fake news. The first one, entitled 'Online participation and crowdsourcing as a solution to mitigate news bias', by Wijekoon et al. addresses the problem of bias in the news and proposes a way to mitigate it. The authors investigate how online participation and crowdsourcing techniques can be utilised to fight against biased news to leverage the power of internet users who are now becoming active participants rather than merely being passive readers. Based on the findings of this study, the authors propose and discuss a novel news platform to mitigate online news bias.

The second paper, entitled 'Combating fake news in social networks through the active participation of users: the approach of EUNOMIA project', by Monachelis et al. proposes that the issue of misinformation in social networks is overcome by encouraging users to participate in a content evaluation process, enabled by the use of a blockchain technology-based tool in a combination of peer-to-peer networks, that can deal with the privacy and ownership of the users. This solution is proposed by the EUNOMIA project, funded under the H2020 research funding program of the EU. The paper presents the architecture adopted in the project, that enables the users to actively engage in the detection of fake news, identify the provenance of information and protect their network from misinformation.

Following are two papers focusing on e-government services. The first, entitled 'Advanced digital skills towards interoperable e-government services: European and Greek case studies', by Stasis and Papastylianou discusses the digital skills policy, frameworks for citizens and professionals, the respective profiles and roles that were developed during the last decade in Europe, focusing on Interoperability. Important case studies such as the National Digital Academy for Citizen in Greece, the ISA Interoperability Academy are being analysed against the above-mentioned frameworks. Additionally, the practices of the Greek National Centre of Public Administration and Local Government, including Open Collaborative Courseware initiatives and a significant reorganisation of the face-to-face courses to online courses, are presented. The results from 147 real cases show that process-based learning can improve service interoperability prospects and enhance interoperability capabilities and competencies in public administration.

The second paper, entitled 'Design issues of a pan European smart cross border 'dream like' e-Gov primary healthcare medical service', by Sideridis et al. discusses design issues of a cross border authentication service, linking public or/and private primary health units. The system in support of this service will offer a standard conceptual design model to interested European Member States. To evaluate the potential of such a system and its practical appeal, Greece's and the UK's primary health care services are examined. These are used as a case study of a conceptual design model applied in building up a pan European smart cross border primary health service to the benefit of citizens of any European countries being on mobility.

The ninth paper of the issue, entitled 'The examination of voter opinions on the implementation and use of i-voting: the case of Poland', by Musiał-Karg and Kapsa presents the results of a survey conducted in Poland between March and May 2018 on

opinions regarding e-voting as a remote voting method. The analysis of demographic features and political preferences highlights differences in opinions on e-voting as a remote voting method. The authors analyse and explain the support for additional election methods among voters in Poland.

In the tenth paper, entitled 'A method for assessing the degree of openness of Semi-Open Data initiatives: applied to the justice domain', Bargh et al. advocate and describe a method to assess the degree of data openness, as a first step for recognising so-called Semi-Open Data initiatives, with a focus on the justice domain. The authors carry out eight case studies, not only to validate the proposed method, but also to show how the method can be deployed in practice.

The last paper of the special issue, entitled 'Revised forensic framework validation and cloud forensic readiness', by Simou et al. proposes a revised version of a cloud forensic-enabled framework that allows to understand the role of the design of forensic-enabled cloud services in a cloud forensic investigation. The forensic requirements of the framework are validated by aligning them with the stages of the cloud forensic investigation process. This alignment facilitates the identification of the degree of the forensic readiness of a cloud service against forensic investigation. The authors applied the framework on a real case scenario to identify the forensic readiness of a company's cloud service.

We are grateful to the authors of the papers in this special issue, for submitting their fine work; to the reviewers that reviewed these papers, and contributed tremendously in improving the content of the issue; and to Prof. Dimitrios Gouscos, IJEG Editor, and Inderscience Publishers, for their support in the process of putting together and publishing this special issue.

We would like to dedicate this special issue to Alexander B. Sideridis, Emeritus Professor of the Agricultural University of Athens, as a small token of appreciation to the man that has dedicated his life to the establishment and advance of informatics in Greece, both in higher education and in government, from a number of positions of high responsibility. Those of us who have had the privilege of having collaborated with him closely value his scientific excellence and contributions to science and to the digital transformation of the country, as well as his wisdom, his integrity and his leadership skills.