COMPUTER LAW & SECURITY REVIEW ■■ (2017) ■■–■■

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Data protection authorities and information technology

Charles Raab [a,*], *Ivan Szekely* [b]

[a] *University of Edinburgh, Scotland, UK*
[b] *Eotvos Karoly Policy Institute, Budapest, Hungary*

Keywords:
Data protection authorities
Supervisory authorities
Privacy
Information technology
General Data Protection Regulation
Survey
Technological competence

A B S T R A C T

The ability of data protection authorities (DPAs) to gain and deploy sufficient knowledge of new technological developments in their regulation of personal-information practices is an important consideration now and for the future. However, DPAs' capacity to keep abreast of these developments has been questionable, and improvements in this are a matter of concern, especially given DPAs' task requirements under the European Union's (EU) General Data Protection Regulation (GDPR). This article reports the findings of a recent survey of EU DPAs that explore the problems they have in comprehending new technologies and how they are dealing with them.

© 2017 Charles Raab & Ivan Szekely. Published by Elsevier Ltd. All rights reserved.

1. Introduction

In the field of information privacy, the overwhelming focus of scholarship for several decades has been on the legal and – increasingly – the technological dimensions of data protection; far less attention has been devoted to understanding the work of regulatory organisations, of which data protection authorities (DPAs) are the most prominent. Nevertheless, the efficacy of legal regimes for protecting personal data relies heavily on the way DPAs perform their tasks, and arguably more than on the letter of the law as seen in statutes and in the connoisseurship of legal scholars. Countries are frequently criticised for only passing laws to protect privacy without also creating implementation machinery that gives the law force through the institutional machinery by means of which compliance, good practice, and other requisites can be encouraged or required; the US is the most prominent case-in-point. Privacy law 'on the ground' rather than 'on the books', in the terms used by Bamberger and Mulligan (2015) in their study of corporate privacy behaviour, involves not only the work of chief privacy officers (CPOs) but of DPAs, with whom those non-state actors frequently engage in relationships that may only be structured vaguely by what the laws say 'on the books'. DPAs play a major role in arbitrating the degree of information privacy that we enjoy as a fundamental right. Their institutional arrangements, provenance, independence, and performance are crucial to that enjoyment, but are less frequently, less systematically, and less comparatively investigated than many of the other components of data protection regimes.

DPAs are multi-taskers. Describing them as 'supervisory authorities', as is done in the European Union's (EU) General Data Protection Regulation (GDPR) (2016), or as 'regulatory authorities', only hints vaguely at one element of the range of activities that they are legally required to do and – less formally – that they are expected to do in the eyes of politicians, the public, and the mass media. Flaherty's (1998, p. 175) inventory of DPAs' includes 'oversight, auditing, monitoring, evaluation, expert knowledge, mediation, dispute resolution, and the balancing of competing interests'. With greater simplification, Jóri (2015) draws attention to two functions: 'shaping' (privacy advocacy) and 'applying' (mediating or enforcing). Referencing

* *Corresponding author*. Politics and International Relations, School of Social and Political Science, University of Edinburgh, Chrystal Macmillan Building, 15a George Square, Edinburgh EH8 9LD, Scotland, UK.
E-mail address: c.d.raab@ed.ac.uk (C. Raab).

http://dx.doi.org/10.1016/j.clsr.2017.05.002
0267-3649/© 2017 Charles Raab & Ivan Szekely. Published by Elsevier Ltd. All rights reserved.

decisions of the European Court of Justice, Schütz (2012) highlights the independence of DPAs and its importance for regulatory functions. Bieker (2017) also mentions this, but focuses upon some forthcoming changes wrought by the GDPR and describes enforcement, complaints-handling, and co-operation across DPAs. The wide-ranging and deep discussion of DPAs by Hijmans (2016, pp. 347–412) considers them as 'expert bodies', but only mentions in passing the relationship between technical knowledge and that expertise. He also points out the way in which the multiple roles of DPAs may involve them in conflicts and compromise their core, compliance-related task, although it is that multiplicity that has made them strong actors in the protection of information privacy.

The survey conducted by the Estonian DPA about the detailed competence and activities of European DPAs distinguishes the following categories: General competence (in the area of personal data protection and in freedom of information matters); educational and consultative activities (answering questions, adoption of guidance texts, approval of self-regulatory acts, training sessions and other public events, media work, including social media); supervision and enforcement activities (mediation, comparative survey, notice without investigation, preventive audit, registration, authorisations regarding data transfer to 3rd countries, prior checking, investigation and resolving of infringements, resolutions); policy advising, and additional activities.[1] Article 57(1) of the GDPR lists twenty-two 'tasks' that Member States' supervisory authorities are required to carry out, ending with the omnibus task 57(1)(v), 'fulfil any other tasks related to the protection of personal data'. This extraordinary range demands activity to be conducted under some twenty-six specified powers (investigative, corrective, authorisation and advisory) conferred under Article 58. Under the GDPR, there are new role requirements or role expectations, a new impetus towards co-operation and institutionalised or informal interaction, but layered on top of the older inventory of roles. The complete 'package' will no doubt require new skills, new resources, and new uncertainties as DPAs face a future in which the possibility of regulation, and thus of protecting people's data and rights, is challenged by new patterns of data processing and new uses for personal data.

Bennett and Raab's (2006, pp. 133–143) pastiche categorisation of what DPAs do outlines seven major tasks, or roles, in which these authorities are engaged as they implement law and oversee practice: ombudsman, auditor, consultant, educator, policy adviser, negotiator, and enforcer. This disaggregation of the institution of a DPA was not intended to be a definitive and universally found catalogue of activities performed by DPAs, much less to imply that all DPAs' performances were necessarily similar. However, it served as an analytical instrument for investigating what DPAs do and how they do it. Some DPAs might emphasise enforcement; others might concentrate on educating the public ('data subjects') and companies or other organisations ('data controllers'). Some are more closely involved than others with advising on policy and legislation, or with negotiating such instruments as codes of practice. Thus the styles and strategies of DPAs in their regulatory roles are not uniform across the landscape of European or global data protection.

What is uniform, however, is their need to understand the data protection and information privacy implications of globally used information and communication technologies (ICTs), large-scale analysis of personal data by a variety of interests, and emerging technologies such as emotion-detection and predictive data analytics. Nearly thirty years ago, before the dawn of the modern Internet and, since then, the further dramatic advances in ICTs and their exploitation by states and private companies, Flaherty noted that DPAs 'monitor and evaluate new technological developments in data processing and telecommunications. Each agency has specialists in various types of information systems and data flows who can speak intelligently about data protection and security with the operators of government information systems' (Flaherty, 1989, p. 383). In 1983, Simitis (1983, p. 177) similarly wrote that these authorities 'have the necessary knowledge enabling them to analyse the structure of public and private agencies and to trace step by step their information procedures. They can therefore detect deficiencies and propose adequate remedies'.[2] Perhaps that was true of the relatively few DPAs at that time in the larger countries of the EU,[3] but is it still the case today, when the technological explosion, the proliferating demands placed upon DPAs, and the growth in their numbers across the EU at national and sub-national levels cast some doubt on their ability to deploy such knowledge in their activities 'on the ground'?

Based on the EU-funded PHAEDRA II project, Barnard-Wills (2017) examines this issue in the context of exploring the possibility of an institutionalised 'technology watch' or foresight capability across EU DPAs, building upon existing but fragmented activity, and referring both to the new co-operation requirements mandated by the GDPR. Semi-structured interviews with DPAs conducted in PHAEDRA II, as well as documentary analysis, showed the variable extent of ICT-related understanding and activity amongst DPAs and elicited explanations for these levels. The separate investigation reported in the present article aims to provide further and somewhat complementary statistical information on the current picture and on the reasons underlying the patterns revealed by DPAs' answers to a questionnaire-based survey of their attitudes and practices.

2. The survey and its methodology

This article attempts to cast light on this subject by reporting the findings of an empirical survey of all EU DPAs that was conducted in late 2015 and early 2016. The survey was organised to coincide with a public panel discussion on DPAs' understanding of ICT that was chaired and moderated by the authors in the Computers, Privacy and Data Protection (CPDP)

[1] http://www.aki.ee/en/inspectorate/typology-dpa-s

[2] Quoted in Flaherty (1989): 383, note 33.

[3] Research conducted in the 1990s by one of the authors suggests that the UK's Office of the Data Protection Registrar, the precursor of the Information Commissioner's Office that operated under the 1984 Data Protection Act and was headed by a computer scientist, nevertheless had only a limited and intermittent in-house capability to keep abreast of ICT development and use in the organisations it regulated.

Please cite this article in press as: Charles Raab, Ivan Szekely, Data protection authorities and information technology, Computer Law & Security Review: The International Journal of Technology Law and Practice (2017), doi: 10.1016/j.clsr.2017.05.002

Download English Version:

https://daneshyari.com/en/article/4957900

Download Persian Version:

https://daneshyari.com/article/4957900

Daneshyari.com