Individual Rights and Information in EU Public Law

Herwig C.H. Hofmann

DRAFT paper for discussion in Upsala 25-26 October 2016 – Not for publication

1. Introduction

In this paper, I will use the occasion of the 250th anniversary of the Swedish freedom of the press act, one of Europe's and most likely the world's first legislative act specifically dedicated to law of information,[1] to review the state of affairs of individual rights relating to information on the EU level and trace the ongoing developments.

The relevance of this precedent and the ongoing discussions surrounding these issues is linked not only to the importance of rights of access to information as tool of accountability as well as data protection as tool for protecting privacy of free individuals in society. The importance of this debate is being increased in today's world through the rising relevance and value of information as the raw material of decision-making.

Individual rights relating to information include the protection of privacy and data protection as well as access to information and transparency provisions. Although information has always had this function, as any reader of Max Weber's considerations on the role of information and expertise in burocracies can attest, within a digitalising world, the relevance of information in everyday life appears to be ever increasing. This is obviously not limited to the public sphere, it is a general societal phenomenon in which the amount of information which is being produced is steadily rising so far at an

[1] Konglige Majestäts Nådige Förordning, Angående Skrif- och Tryck-friheten of December 2, 1766.

exponential rate. Economiccally, the role of information is rising with the process of digitalisation of societies and of the spread of networked devices and services and the process of transformation from goods-based to service-based economies (such as with music, films, software etc.). Information-based businesses offering search engines and social media concentrate big amounts of market power but these are also coerced to share their information with public actors. At the same time, the information society produces an abundance of information which is produced which awaits beign combined in new and creative ways for the general good in a great diversity of fields such as to improve environmental protection, health protection, distribution of social benefits, whether previsions, financial forecasting, investment decisions, as well as information useful about national security and policing decisions to name just a few. By comparison to the situation 250 years ago in Sweden, this gives a new dimension to an old problem. In any case, the effects are relevant for understanding the role of individual rights in a digitalised society in which tracking of individual habits, identification of prefences and personality traits, assessment of intellectual abilities, health data, sexual orientations as well as poltical and societal interests is now easily possible even without the knowledge and consent of the data subject and is regularly undertaken by various public and private actors.

Therefore, in a world in which information is becoming ever more relevant and prevalent, societies need to take key decisions about how to address information-related legal questions. Such value choices were the basis of the Swedish law of 1766 abolishing censorship and granting access to official documents. Its purpose was to encourage the free exchange of ideas in order to achieve what we would call today a society based on democracy and individual rights.[2] Today, however the questions related to information relevant to democracy in a digitalised information society,[3] also include issues such as the ownership of data and information wilfully or incidentially 'emitted' by individuals, possibilities of public and private handling of data, rules of public access and accessability of information, questions of knowledge about existing data and data collection tools as

[2] Importantly, this legislation was developed as the Swedish contribution to democratic socieites under the rule of law in a historic period full of constitutional turmoil such as the French and the American revolution which altogether have changed our understanding of the role of the individual in a constitutionalised society.

[3] For a discussion of one possible conceptualisation of an information society see Manuel Castells, *The Rise of the Network Society, The Information Age: Economy, Society and Culture* (Oxford: Blackwell, 2006).

well its distribution, possible deletion and correction. These big issues have huge implications for such central value orientations in society as the concept of a self-determined individual, the possibility of effective democratic participation, the concentration and possible separation of powers, the balance between public and private powers and many others more. Implicitly, this was an underlying concern some 250 years ago in the debates leading to the Swedish legislation of 1766. Digitalisation of socieites makes these issues all the more pressing issue today.

The relevance of individual information rights for the role of the individual in a democratic society under the rule of law, tracable all the way back to the Swedish legislation of 1766 and its reasoning remains visible until today. Not only because of the great importance of EU law for all its Member States, and given the great influence the Swedish accession to the EU in 1995 has had in respect to developing a sensitivity for information law in the EU, the question arises where EU law stands with respect to the core cornerstones of information law today – especially with regard to those elements of information law relating to individual rights.

But before entereing into the discussion and evaluation of the EU's rules on law of information, it is worth understanding the **spectrum of regulatory possibilities** in which the decisions about privacy or access, ownership or limitation of information is made. Technically speaking, it might appear that full openness and accessibility of information – both emanating from public and private sources – should or at least could be the default option of the digital, internet-based world. By comparison in a pre-digital world, and this makes the approach to openness within the Swedish law of 1766 all the more remarkable, non-accessibility of information, irrespective of whether public or private would have appeared as the norm not least for the difficulties involved of accessing such information. Further considerations illustrate the spectrum: With relation to law of information, the 'ideal' of a totalitarian system would appear to consist of maintaing secrecy about information in the hands of public powers, whilst having unlimted access to all information in the private domain. On the other hand, the ideal of a democratic system under the rule of law, should be closer to a concept of transparency

and accessability of information by public bodies whilst maintaining privacy of the private individuals.

This paper will look at where EU law on information currently fits within this spectrum of possibilities and how in EU law the balancing is been currently undertaken. In order to make things slightly more operational, I will put a focus on case law relating to the protection of personal data and privacy, on one hand, and the protection of access to documents, on the other. The paper is based on excerpts of my 2011 book written together with Gerard Rowe and Alexander Türk (Administrative Law and Policy of the EU) updated with some of the highly relevant case law and developments of the past 5 years. This paper is a basis for discussion only.

2. Individual rights and information in the EU – an overview

The main cornerstones in the protection of individual rights regarding information in EU law are Articles 7 and 8 of the Charter of Fundamental Rights of the EU (CFR) for privacy and the protection of personal data (also in Art. 16(1) TFEU and Article 39 TEU) as well as in Articles 42 CFR for general access to documents (also in Art. 15 TFEU as well as with regard to one's file Art. 41 (2) b CFR).

Article 7 CFR protects 'the right to respect for his or her private and family life, home and communications'. The scope of this article *inter alia* protects with respect to the home and the communications protection essentially against physical or electronic searches. Article 8(1) CFR grants the 'right to the protection of personal data concerning him or her' and Article 8(2) specifies that 'data must be processed fairly for specified purposes and on the basis of the consent of the persons concerned or some other legitimate basis laid down by law.' The CJEU reads Articles 7 and 8 CFR together when reviewing the right of privacy and data protection.[4] This 'joint' right has a personal scope covering both legal and natural persons, in line with case law of the ECtHR.[5] Protection is offered under

[4] Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* EU:C:2010:662, para 85; Joined cases C-293/12 and C-594/12 *Digital Rights Ireland* (Grand Chamber) ECLI:EU:C:2014:238 of 8 April 2014, para 29.
[5] ECtHR *Amann v. Switzerland*, § 65; ECtHR *Rotaru v. Romania*, § 43.

these rights against processing of processing of 'personal data by a third party' concerning 'any information relating to an identified or identifiable individual.'[6]

Privacy and Data Protection are protected by the CJEU as central elements to a democratic society in which public access to information and the use of such information about individuals is strictly limited by law. The links between Arts 7 and 8 CFR were first developed in the case law of the ECtHR regarding Art 8 ECHR and the adoption of the concept of the right to 'informational self-determination' (*informationalle Selbstbestimmung)* first developed by the German Constitutional Court in the late 1970ies and early 1980ies. The underlying concept is, simply described, that data about a person on emitted by a person (e.g. phone raoming information, internet browsing history etc) is akin to the persons's property. Any access can be in principle regarded an infringement of the right.

The requirement in Article 8(3) CFR that data protection be ensured by an 'independent authority' is a particularity in EU fundamental rights law which can be said to have its origins in another particularity of Swedish law, especially the creation of the person of the independent Ombudsman in 1809 in charge also of enforcement of rights arising from the 1766 act.

Transparency rights are both to be found with respect to the right to access of one's own file in
Art. 41 (2) b CFR as well as the more broad right of access to Documents in Art. 42 CFR and Article 15 TFEU. The right of access to one's file has been accepted as General Principle of EU law since the early days of the E(E)C. In *SNUPAT* the CJ held that 'it would infringe a basic principle of law to base a judicial decision on facts and documents of which the parties, or one of them, have not been able to take cognizance and in relation to which they have not therefore been able to formulate an opinion'[7]

Regarding the general right of access to documents, Art. 15 TFEU explains that this right exists explicitly to 'promote good governance and ensure participation of the civil

[6] Case C-291/12 *Schwarz* ECLI:EU:C:2013:670 of 17 October 2013, paras 24-26 - a case on biometric details in passports.
[7] Cases 42 and 49/59 *S.N.U.P.A.T. v High Authority* [1961] ECR 103, 172 (summary point 1).

society'. It is also a guarantee of the rule of law and democracy by allowing real supervision of public action.

3. Where is EU law heading to with respect to the privacy and data protection?

Freedom of information and access to documents

Freedom of information, or more narrowly, the right of access to documents, has not always been regarded as a fundamental right, or even a matter of priority in European administrative law. In line with the administrative traditions of many European countries, public non-accessibility and secrecy were generally the norm in regard to information held by European authorities.[8] This approach changed gradually in the light of the increasing recognition of the individual's right to information as a basis of both a fair, accountable, and transparent administration and a functioning, participatory democracy in which citizens were permitted to engage in an informed debate and to exert influence on public decision-making.

Important impulses for the development of freedom of information in the EU came with the 'Nordic' enlargement of 1995 which gave the Swedish and Finnish traditions in this area a strong influence in the EU.[9] The idea of freedom of information as a means of fostering freedom of expression, transparency, and participation, as well as accountability

[8] See eg Case C-170/89 *BEUC v Commission* [1991] ECR I-5709 in which the consumer protection NGO, BEUC, was denied access to non-confidential elements of Commission files in an anti-dumping case.

[9] See eg Section 12 of the Finish constitution of 1999 which expressly links freedom of expression and the right of access to information: 'Everyone has the freedom of expression. . . . Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.' See the unofficial translation of the Finish constitution of 1999 on the finlex website (<http://www.finlex.fi>). This provision has been described as having a lineage dating back to 18th-century Swedish legislation at the time applicable in Finland. See for further references, Paivi Leino, 'Comment on Case C-353/99 P', *CMLRev*. 39 (2002) 621–32. See, for an historic analysis of the development of the right to access to information, eg Deirdre M. Curtin, 'Citizens' Fundamental Right to Access to EU Information: An Evolving Digital Passepartout?', *CMLRev*. 37 (2000) 7–41 at 7–11; Peter Dyrberg, 'Accountability and Legitimacy: What is the Contribution of Transparency?' in Anthony Arnull and Daniel Wincott (eds), *Accountability and Legitimacy in the European Union* (Oxford: Oxford

and good administrative governance in general, has consequently taken increasing hold even in Member States which did not originally subscribe to this approach.[10]

The right of access to documents is now protected both as a general principle of European law and through provisions of EU primary law. Article 15(3) TFEU (slightly expanding Article 255(1) EC), lays down that:

> [a]ny citizen of the Union and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union institutions, bodies, offices and agencies, whatever their medium, subject to the principles and the conditions to be defined in accordance with this paragraph.

This formulation implements in the TFEU the expression contained in Article 42 CFR, which since its beginning included a right of access to documents. Article 15(3) TFEU explicitly provides access to documents not only of institutions but also of bodies and agencies. The right of access to documents has, over the years, also been an element of several generations of regulation in secondary law.[11] Regulation 1049/2001 issued on the basis of Article 255 EC (now Article 15 TFEU) is the general legislation on access to documents.[12] An exception is the field of environmental law which profits from a more open approach through the specific implementation of the Aarhus Convention.

Attitudes toward granting access to information are occasionally hostile in the EU's and the Member State executives. An example is that under Protocol (No 36) to the Treaty of Lisbon, policy matters arising from the former Second and Third Pillars were covered, for

---

University Press, 2002) 81–96 at 86–92; Inger Österdahl, 'Openness v Secrecy: Public Access to Documents in Sweden and the European Union', *ELRev.* 37 (1998) 336–56; all with further references.

[10] By the year 2000, nearly all of the then 15 Member States had introduced a Freedom of Information Act. (See for a comparative overview of the situation in 2001, the opinion of Léger AG of 10 July 2001, paras 55 and 80, 81 in Case C-353/99 P *Council v Hautala* [2001] ECR I-9565.) This was not least due to the influence of a Europeanization of national administrative rules in the context of an increasingly integrated administration in the EU. See above in Chapter 1. For a comparative overview of EU and Member State rules see, Herke Kranenborg and Wim Voermans, *Access to Information in the European Union* (Groningen: Europa Law Publishing, 2005) 10–27.

[11] Initially, the institutions had adopted internal guidelines. Original decisions of the institutions (Council Decision 2001/840, OJ 2001 L 313/40; Commission Decision 2001/937, OJ 2001 L 345/94; EP Decision 2001/2135, OJ 2002 C 140E/120) were based on the right to self-organization.

five years after the entry into force of that Treaty, by the former specific rules established for those regimes. For this reason, on the last day prior to entry into force of the Lisbon Treaty, the Council passed a host of legislation in a last-ditch attempt to bar the European Parliament from legislating with respect to these essential procedural fundamental rights at least during the transition period, that is, until 30 November 2014.

The main instrument for ensuring access to information in the EU remains to date Regulation 1049/2001.[13] Its stated purpose is 'to promote good administrative practice on access to documents' by proclaiming the principle of 'the fullest possible exercise of the right of public access to documents'.[14] Under its provisions, the Council, the Parliament, and the Commission and, by extension, European agencies will grant access to documents in their possession regarding the EU, the former EC, and Euratom matters.[15] Documents are defined as 'any content whatever its medium . . . relating to the policies, activities and decisions falling within the institution's sphere of responsibility'.[16] The GC has expanded this to documents arising from comitology committees, finding that for these documents, the Commission is obliged to grant access.[17] Although Article 15 TFEU and Article 2 of Regulation 1049/2001 grant the right of access to 'any citizen of the Union' and any natural or legal person residing or registered in a Member State, the institutions' guidelines enlarge this scope by allowing applications for access to documents irrespective of nationality or place of residence.[18]

Access will be granted by EU institutions not only to documents drawn up by themselves, but also documents received by them. In this regard, Declaration No 35 attached to the Final Act of the Treaty of Amsterdam incorporated the right of an institution to refuse

---

[12] Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001 L 145/43.

[13] See with further explanations Bart Driessen, 'The Council of the European Union and access to documents', *ELRev.* 30 (2005) 675–96; Magdalena Elisabeth de Leeuw, 'The Regulation on public access to European Parliament, Council and Commission documents in the European Union: are the citizens better off?', *ELRev.* 28 (2003) 324–48.

[14] Art 1(a)–(c) Regulation (EC) 1049/2001.

[15] Arts 28(1) and 41(1) EU; Declaration 41 attached to the Final Act of the Treaty of Amsterdam; Regulation (EC) 1049/2001, considerations 5, 6, 8.

[16] Art 3 of Regulation (EC) 1049/2001.

[17] Case T-188/97 *Rothmans v Commission* [1999] ECR II-2463, para 62.

[18] EU, *Access to European Parliament, Council and Commission documents—a user's guide* (Luxembourg: Office for Official Publications of the European Communities, 2002) 13.

permission to communicate to third parties documents originating from Member States. Accordingly, Article 4(5) of Regulation 1049/2001 grants Member States the right to veto disclosure.[19] This veto power is, however, is limited. In a Grand Chamber decision, the CJ held that:

> [an] institution cannot accept a Member State's objection to disclosure of a document originating from that State if the objection gives no reasons at all or if the reasons are not put forward in terms of the exceptions listed in Article 4(1) to (3) of Regulation No 1049/2001. Where, despite an express request by the institution to the Member State to that effect, the State still fails to provide the institution with such reasons, the institution must, if for its part it considers that none of those exceptions applies, give access to the document that has been asked for.[20]

A similar parallel application of general access rules and policy-specific provisions has been established by the so-called Aarhus Regulation on access to environmental information.[21] Its provisions are more far reaching than those of Regulation 1049/2001. Thus, where information is related to environmental issues as provided for in the Aarhus

---

[19] The European institutions are bound by the refusal of a Member State to grant access to documents, see Case T-168/02 *IFAW Internationaler Tierschutz Fonds v Commission* [2004] ECR II-4135, paras 55, 57, 58; Case T-187/03 *Scippacercola v Commission* [2005] ECR II-1029, para 56. They may not enter into a review of responsibilities of the Member States. Case T-76/02 *Messina v Commission* [2003] ECR II-3203, para 46: 'It is not for the Commission to rule on the division of competences by the institutional rules proper to each Member State'. Further, they may not ask the Member State for reasons for the refusal, see Case T-168/02 *IFAW Internationaler Tierschutz Fonds v Commission* [2004] ECR II-4135, para 59. For a discussion of this notion, see Pedro Cabral, 'Access to Member State Documents in EC Law', *ELRev.* 31 (2006) 378–89; Bart Driessen, 'Access to Member State documents in EC Law: a comment', *ELRev.* 31 (2006) 906–11.

[20] Case C-64/05 P *Sweden v Commission* [2007] ECR I-11389, para 88.

[21] Regulation (EC) 1367/2006 of the European Parliament and of the Council of 6 September 2006 on the application of the provisions of the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies, OJ 2006 L 264/13. This measure brings to force within the Community obligations from the United Nations Economic Commission for Europe (UNECE) Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters (the Aarhus Convention). The Community approved the Aarhus Convention on 17 February 2005 by Council Decision 2005/370/EC, OJ 2005 L 124/1. The regulation needs to be read in connection with the environment information and participation directives, aimed at harmonizing Member States' approaches in these fields: the Environmental Information Directive 2003/4/EC on public access to environmental information and repealing Council Directive 90/313/EEC, OJ 2003 L 41/26 as well as Directive 2003/35/EC providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC—Statement by the Commission, OJ 2003 L 156/17.

Convention, which the regulation implements, those more widely ranging rights of access can be invoked in parallel with any generally applicable ones.[22]

Limitations on the right of access to documents arise from primary law provisions such as Article 339 TFEU protecting professional secrets, as well as from secondary law. Although under the case law of the European courts, exceptions to the right of access must, in principle, be construed and applied restrictively, so as not to defeat the general principle enshrined in primary and secondary law.[23] Case law fo the CJEU has become rather open to broad and sweeping exceptions.

Basically, the Regulation contains two types of exceptions, mandatory and conditional. Mandatory exceptions oblige the administration to 'refuse access' where specified circumstances obtain.[24] Conditional exceptions are those where the institution shall refuse access 'unless there is an overriding public interest in disclosure',[25] in other words, where there is an exception to the exception. In any case, the risk of a protected interest being undermined must be 'reasonably foreseeable and not purely hypothetical'.[26] Since an applicant for access to documents does not need to state his or her interest in obtaining this,[27] an institution may in principle not take an applicant's interest into account when concluding that there are mandatory reasons for refusing the application under Regulation 1049/2001.[28] A refusal under one of the exceptions must be based on a concrete analysis of the content of the document. Where an institution receives a request 'it is required, in principle, to carry out a concrete, individual assessment of the content of the documents referred to in the request', and partial access is to be granted where an exception is

---

[22] In reality the distinction may cause some problems especially with respect to 'plans and programmes relating to the environment' which, under consideration 9 of the Aarhus Regulation, are defined in an encompassing way.

[23] Standing case law, see eg Case T-211/00 *Kuijer v Council* [2002] ECR II-485, para 55; Case T-20/99 *Denkavit Nederland v Commission* [2000] ECR II-3011, para 45; Joined Cases C-174 & 189/98 P *Netherlands and van der Wal v Commission* [2000] ECR I-1, para 27.

[24] Art 4(1) of Regulation (EC) 1049/2001.

[25] Art 4(2) and (3) of Regulation (EC) 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, OJ 2001 L 145/43.

[26] Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, para 115.

[27] Art 6(1) of Regulation (EC) 1049/2001, which explicitly states that 'the applicant is not obliged to state reasons for the application'.

[28] Joined Cases T-110, 150 & 405/03 *Sisón v Council* [2005] ECR II-1429, paras 50–52; confirmed in Case C-266/05 P *Sisón v Council* [2007] ECR I-1233, paras 62–64, 80–83; Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, para 82; Case T-124/96 *Interporc v Commission (Interporc I)* [1998] ECR II-231, para 48; Case T-92/98 *Interporc v Commission (Interporc II)* [1999] ECR II-3521, para 44.

relevant only to parts of the document.[29] It should be noted that requests for large amounts of documents and requests for wide-ranging information not readily available in the administration have been the subject of dispute.

So far the principle, in reality of the past years a quite different picture emerges. The exceptions within the second category also include documents drawn up in the context of court proceedings[30] or in relation to the provision of internal legal advice. The Court has interpreted this exception as meaning 'documents drawn up *solely* for the purposes of *specific* court proceedings',[31] placing the latter explicitly within the context of safeguarding the professional secrecy of the institutions' in-house or external legal counsel.

Further, the types of documents falling into the second category include documents needed for the 'purpose of inspections, investigations and audits', as well as documents 'drawn up by an institution for internal use or received by an institution'. The latter relates to a matter where the final decision has not (yet) been taken by the institution, and where such disclosure 'would seriously undermine the institution's decision-making process'.[32] The GC has limited the possibility for the institutions to limit access to documents under the exception relating to an inspection or investigation, such documents being covered by the exception only so long as the investigations, inspections, or audits continue.[33] The Court further qualified the scope of the exception, finding that to allow limitation of access:

> until the follow-up action to be taken has been decided would make access to the documents dependent on an uncertain, future and possibly distant event, depending on the speed and diligence of the various authorities. Such a solution would be contrary to the objective of guaranteeing public access to documents

[29] Case T-2/03 *Verein für Konsumenteninformation v Commission* [2005] ECR II-1121, paras 66–74; Case T-14/98 *Hautala* [1999] ECR II-2489, paras 28 and 82.

[30] Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, para 89; Case T-92/98 *Interporc v Commission (Interporc II)* [1999] ECR II-3521, para 40.

[31] Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, para 90 (emphasis added). See also Case T-92/98 *Interporc v Commission (Interporc II)* [1999] ECR II-3521, para 41, emphasis added in the text. With the latter, Regulation (EC) 1049/2001 establishes the protection of institutions' legal advice, which the courts had been slow to accept for private parties' legal counsel. See also Case 53/85 *AKZO Chemie v Commission (AKZO II)* [1986] ECR 1965, para 26.

[32] Art 4(2) and (3) of Regulation (EC) 1049/2001.

[33] Case T-20/99 *Denkavit Nederland v Commission* [2000] ECR II-3011, para 48.

> relating to any irregularities in the management of financial interests, with the aim of giving citizens the opportunity to monitor more effectively the lawfulness of the exercise of public powers.[34]

Within the second category as a whole, access may be limited unless there is an overriding public interest in disclosure. The overriding public interest must be the interest of the public in general. This results from the fact that the purpose of the regulation is to guarantee access for everyone to public documents, not merely access for the requesting party to documents which concern it. Consequently, the particular interest which may be asserted by a requesting party in obtaining access to a document concerning it individually cannot be taken into account.[35] An overriding public interest, however, must go beyond the normal public interest in disclosure of information as protected in Regulation 1049/2001 reflecting the principles of openness, democracy, and greater citizen participation of in the decision-making process:

> If that is not the case, it is, at the very least, incumbent on the applicant to show that, having regard to the specific facts of the case, the invocation of those same principles is so pressing that it overrides the need to protect the document in question.[36]

This was confirmed by the CJEU in *Sweden and Turco*[37] in which the Grand Chamber ruled on the appeal by Sweden and Mr Turco against a GC confirming a Council decision to refuse access to an opinion of the Council's legal service (on a directive for minimum standards of treatment of Asylum seekers). The question was how the requirement of the 'overriding public interest in disclosure' in Article 4(2) of Regulation 1049/2001[38] can be interpreted. Turco held that the principles of 'democracy and citizen participation in the legislative process' in themselves constitute an overriding public interest. The Council claimed a 'space to think' to maintain internal advice confidential. The interests quoted by Turco are the general interests already taken into account by Reg 1049/2001 and not

---

[34] Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, paras 109–112; Case T-123/99 *JT's Corporation v Commission* [2000] ECR II-3269, para 50.

[35] Joined Cases T-391/03 & T-70/04 *Franchet and Byk v Commission* [2006] ECR II-2023, paras 136–138. In this case, the general interest which the applicants claimed was the right to a fair hearing. The Court found that although the right to a fair hearing is in itself a general interest, the fact that this right was manifested in the present case by the applicants' individual interest in defence implied that the interest which the applicants invoked was not a general, but rather a private, interest.

[36] Case T-84/03 *Turco v Council* [2004] ECR II-4061, summary point 3 and paras 80–83.

[37] Case C-39/05 P and 52/05 P *Sweden and Turco v Council* of 1 July 2008 (Grand Chamber).

[38] "The institutions shall refuse access to a document where disclosure would undermine protection of … court proceedings and legal advice, unless there is an overriding public interest in disclosure".

specific ones additional to that. The General Court[39] had held that any exception "must be interpreted strictly" but the effet utile of Art 4(2) Reg 1049/2001 would be undermined if any public interest in disclosure could override the principled confidentiality of internal legal advice. The Court of Justice by contrast found that Article 4 of the Regulation 1049/2001 is an expression of the 'right of public access to documents of the institutions' 'is related to the democratic nature of those institutions.'[40] Refusal of access must therefore be assessed on a case by case basis and exceptions to the principle of access must be interpreted strictly.[41] In any case, any 'risk to the Council's decision making process must be "reasonably foreseeable and not purely hypothetic.'[42] The Court however adds that the considerations made 'are clearly of particular relevance where the Council is acting in its legislative capacity…' since the 'openness in that respect' and 'the possibility for citizens to find out the considerations underpinning legislative action is a precondition for the effective exercise of their democratic rights.'[43]

This approach which appears rather sympathetic to the principles of openness and access to documents however appear in a very different light when seen applied to administrative procedures as opposed to a legislative procedure as was the case in *Sweden* and *Turco*. Reading the Case C-612/13 P *Client Earth* of 16 July 2015 with its plentiful references to earlier case law makes this abundantly clear. *Client Earth* is and environmental NGO attacks the refusal of access to Commission documents on MS compliance with certain EU legal acts. In question is the EU implementation legislation (Reg 1367/2006) of the *Arhus Convention* (an international treaty on public access to environmental information). The Reg finds that in certain cases of Art. 4(2) Reg 1049/2001[44] 'an overriding public interest shall be deemed to exist' e.g. where information relates to 'emissions into the environment.' The Commission had argued that the information sought is protected since it is part of an ongoing investigation (acitivté d'enquête) into MS compliance with EU law and the GC in that case had sided with the Commission.[45] The Court of Justice then found that 'in order to justify refusal of access

[39] T-84/03 *Turco* para 71.
[40] Case C-39/05 P and 52/05 P *Sweden and Turco v Council* of 1 July 2008 (Grand Chamber), para 35.
[41] Case C-39/05 P and 52/05 P *Sweden and Turco v Council* of 1 July 2008 (Grand Chamber), para 36.
[42] Case C-39/05 P and 52/05 P *Sweden and Turco v Council* of 1 July 2008 (Grand Chamber), para 39.
[43] Case C-39/05 P and 52/05 P *Sweden and Turco v Council* of 1 July 2008 (Grand Chamber). Para 41.
[44] Art. 4(2) Reg 1049/2001 allows limiting access to protect ongoing investigations and for the purpose of protecting inspections, investigations and audits unless there is an overriding public interest.
[45] T-111/11 *Client Earth.*

to a document' under Article 4(2), (3) of Reg 1049/2001, the institution 'provide explanations as to how access to that document could specifically and actually undermine the interest protected by an exception laid down in that article.'[46]

The Court of Justice however takes, especially disappoing when looking at the reference to the principle of democracy as guiding principle for interpretation of Article 4(2) of Regulation 1049/2001, the approach that 'disclosure, if it had been authorised, would have been detrimental to the climate of trust which has to exist between the Commission and each MS concerned and would have impeded, in the event that infringements of European law were identified, the achievement, free from external pressure, of a consensual solution.'[47]

After this heavy blow to interpretation of Article 4(2) Reg 1049/2001 in the light of the principle of democracy, the question arises of "what is left of access after *Client Earth?*" The answer is probably, "not much" especially when looking at paragraph 77 of the judgement which *de facto* establishes a judge-made general presumption of confidentiality of documents, as it would appear much in contrast to the telos of Regulation 1049/2001.

> 'The Court has recognised five types of documents which enjoy a general presumption of confidentiality:
>
> - documents in an administrative file relating to a procedure for reviewing **State aid** (see C-139/07 P *Commission* v *Technische Glaswerke Ilmenau* EU:C:2010:376);
> - pleadings lodged by an institution in **court proceedings** (see, C-514/07 P C-528/07 P and C-532/07 P *Sweden and Others* v *API and Commission*, EU:C:2010:541, para 94);
> - documents exchanged between the Commission and notifying parties or third parties in the course of **merger control** proceedings (see C-404/10 P *Commission* v *Éditions Odile Jacob* EU:C:2012:393 para 123);

[46] Case C-612/13 P *Client Earth* of 16 July 2015 with reference *iner alia to* C-365/12 P *Commission* v *EnBW*, EU:C:2014:112, para 64.
[47] Case C-612/13 P *Client Earth* of 16 July 2015, para 41.

- documents concerning an **infringement procedure** during its pre-litigation stage (see C-514/11 P and C-605/11 P *LPN and Finland* v *Commission* EU:C:2013:738, para 65);
- documents relating to a proceeding under **Article 101 TFEU** (see C-365/12 P *Commission* v *EnBW* EU:C:2014:112 para 93).'[48]

The Court then states, maybe in conscience of these far reaching exclusions of the main fields of 'direct administration' o fthe Commission and a sweeping exclusions o fthe Commission's activities as guardian of the treaties under Article 17 TEU, as a consolation prize that 'such a general presumption does not rule out the possibility of demonstrating that there exists, under the last clause of Article 4(2) of Regulation No 1049/2001, an overriding public interest justifying the disclosure of the document concerned.'[49] Nonetheless, Client Earth's claims 'that the principles of transparency and democracy entail that citizens have the right to be informed of the extent to which national law is compatible with European Union environmental law and to participate in the decision-making process' were deemed by the Court as merely consisting of general considerations which 'are not capable of demonstrating that the principles of transparency and democracy raised in this case issues of particularly pressing concern which could have prevailed over the reasons justifying the refusal to disclose in their entirety the contested studies placed in a file relating to the pre-litigation phase of infringement proceedings.'[50]

These limitations weigh especially heavy since freedom of information is one of the central elements of a transparent governance structure and an open society. It contributes to informed participation in, and scrutiny of, public activity by the citizens and interested organizations. Reflecting these aspirations, freedom of information has seen considerable development, especially in the last two decades. Under the influence of Nordic constitutional and administrative traditions, and of international environmental law, the originally rather secretive approach of the European institutions has been shifted largely towards a more open system. Nevertheless, more can be don as becomes especially clear when comparing the general rules on access to documents with those contained in the Aarhus Regulation. In the light of such a comparison, Regulation 1049/2001 appears

[48] Case C-612/13 P *Client Earth* of 16 July 2015, para 77 [bulletpoint listing added].
[49] Case C-612/13 P *Client Earth* of 16 July 2015, para 89.
[50] Case C-612/13 P *Client Earth* of 16 July 2015, para 89 with reference to C-514/11 P and C-605/11 P *LPN and Finland* v *Commission* EU:C:2013:738 para 93, 95; C-127/13 P *Strack* v *Commission* EU:C:2014:2250 para 131.

unnecessarily restrictive, with respect both to the parties enjoying access rights and to the bodies from which the granting of access may be sought. The existing patchwork of access rules is as confusing as it is unnecessary. As the Commission has itself pointed out in its Green Paper on public access to documents held by EC institutions,[51] it is not always easy to discern who has which right to information.

Privacy and Protection of Personal Data

EU law governing information contains not only rules on access but also on the protection of data. According to its understanding in the context of the Union, data protection constitutes an individual right against the potential misuse of information both by governments and non-governmental actors. Such potential for misuse arises, first, through the gathering of such a range and amount of information which, when combined, may allow highly individual, sensitive, and private details to be revealed. It arises secondly, through a subsequent distribution allowing data to fall into the hands of those using it wrongly, indeed illegally. Thirdly, it may emerge through errors in the information itself which may create serious difficulties for those concerned, especially where information exchanged between multiple users may exacerbate the harm to individuals.[52] The function of data protection law is to respond to each of these potentials, as regard both natural and legal persons. In European law, data protection law contains very different rules for each of these categories of persons.

Provisions on data protection had initially been developed in the Member States since the rise of ever more sophisticated information technology has allowed for large-scale data collection, processing, and distribution, especially across information networks.[53]

---

[51] Green Paper: Public Access to documents held by institutions of the European Community, 18 April 2007, COM(2007)185 final.

[52] See, for a good summary of the goals of data privacy (explained in view of the differences between the European and the US approaches), Francesca Bignami, 'Transgovernmental Networks v Democracy: The Case of the European Information Privacy Network', *Mich. J. Int'l L* 26 (2005) 807–68 at 813–19 with further references. See also Spiros Simitis (ed), *Bundesdatenschutzgesetz Kommentar* (Baden-Baden: Nomos, 2006) introduction, 65–6, paras 9–12.

[53] The earliest data protection laws existed in the German State of Hessen (1970), Sweden (1973), Germany's federal level (1977), and France (1978). In 1980, the OECD published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc C 58 of 1 October 1980.

Constitutional provisions in many Member States' reflects this.[54] Early reactions to the development of IT also existed on the level of public international law through the ECHR.[55] In EU law this approach was taken up through the case law of the CJEU and is now established in Articles 7 and 8 CFR.[56] In fact, the development of the protection of fundamental rights protection in the form of general principles of EU law originated in 1969 from a case concerning data privacy in *Stauder*.[57]

Two basic acts of EU secondary law establish the basic rules on the extent and limits of the right to the protection of personal data in those policy areas of the EU which arise from the former EC. The first is Directive 95/46, addressed to the Member States,[58] which is designed to establish a harmonized level of data protection, avoiding potential impediments to the internal market by differing data protection rules.[59] It has been

[54] Mentioned (as right to privacy or explicitly to data protection) in eg Art 22 of the Belgian Federal Constitution; Art 38 of the Bulgarian Constitution; Arts 3, 112(1) of the Czech Constitution; Art 10 of the Dutch Basic Law; Art 42 of the Estonian Constitution; Art 9(1) of the Greek Constitution; para 10(1) of the Finnish Constitution; Art 59 of the Hungarian Constitution; Art 2(1) in combination with Art 1(1) of the German Federal Basic Law; Art 51 of the Polish Constitution; Art 26(2) of the Portuguese Constitution; Arts 19(3) and 22(1) of the Slovakian Constitution; Art 38 of the Slovenian Constitution; Chapter 2, para 3 of the Swedish Constitution.

[55] In 1981, the Council of Europe adopted the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with Regard to Automatic Processing of Personal Data, 1981, ETS No 108. This convention entered into force on 1 October 1985 and currently has 38 Members. An Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No: 181, entered into force on 1 July 2004 so far has 15 signatory states.

[56] See Art 8 ECHR, 'Everyone has the right to respect for his private and family life, his home and his correspondence'; Art 8 CFR, '(1) Everyone has the right to the protection of personal data concerning him or her. (2) Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. (3) Compliance with these rules shall be subject to control by an independent authority.' See also Veith Mehde, 'Datenschutz' in Sebastian Heselhaus and Carsten Nowak (eds), *Handbuch der europäischen Grundrechte* (Munich/Vienna/Bern: Beck, 2006) 610–11, paras 4–6; Spiros Simitis (ed), *Bundesdatenschutzgesetz Kommentar* (Baden-Baden: Nomos, 2006) introduction, 118–29, paras 151–83.

[57] Case 29/69 *Stauder v Stadt Ulm* [1969] ECR 419. Ironically, Erich Stauder, who went to court to enforce his right to privacy and won the case, consequently has become the best known name in the history of fundamental rights protection of the EC.

[58] For details see Spiros Simitis (ed), *Bundesdatenschutzgesetz Kommentar* (Baden-Baden: Nomos, 2006) introduction, 136–47, paras 203–32; Veith Mehde, 'Datenschutz' in Sebastian Heselhaus and Carsten Nowak (eds), *Handbuch der europäischen Grundrechte* (Munich/Vienna/Bern: Beck, 2006) 615–17, paras 16–18; Herbert Burkert and Ulf Brühann, 'Europarechtliche Grundlagen' in Alexander Rossnagel (ed), *Handbuch Datenschutzrecht* (Munich: Beck, 2003) 102–11, paras 44–63 and 135–48, paras 15–55.

[59] 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, OJ 1995 L 281/31.

replaced by Regulation 2016/679,[60] which apply as of May 2018. The Directive as well as its replacement, the Regulation apply 'to the processing of personal data".[61] The approach taken is to understand data protection as a right of defence against state action as well as against private misuse of data. Both the Directive and the Regulation exclude from their scope data processing in matters of foreign and security policy as well as those relating to 'public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law'.[62] Therefore, a new regulation

The processing of personal data by EU authorities is regulated in a separate regulation, which is currently under review, Regulation 45/2001,[63] applies to collection and processing of data by Union authorities. Under Regulation 45/2001, authorities are obliged when handling personal data to process these only for a specific and legitimate reason, to be stated when the data are collected. The individual concerned has the right to obtain access to the data, to have it rectified, blocked, or erased under the conditions set out in the provisions, and finally has the right to object to its processing under certain circumstances.[64] Enforcement and supervision of these rights and obligations is undertaken in a layered system. Each Union institution and body appoints an internal 'data protection officer' who is responsible for ensuring, in an independent manner, that the regulation is applied within the organization concerned.[65] The data protection officer keeps *inter alia* a register of the data-processing operations carried out by the organization. Each organization's data protection supervisor cooperates with the EU's external 'independent supervisory authority', the European Data Protection Supervisor (EDPS).[66]

---

[60] 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), OJ 2016 L 119/1

[61] Art 1 of Regulation 2016/679 and Article 3(1) of Directive 95/46/EC.

[62] Art 3(2) of Directive 95/46/EC.

[63] See specifically Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001 L 8/1, discussed below.

[64] Arts 13–18 of Regulation (EC) 45/2001.

[65] Art 24.

[66] Arts 41–48. The EDPS was created under the mandate of the former Art 286 EC, which has now been reformulated as Art 16(2) TFEU. For a detailed description of the procedures and activities of the EDPS, see Hielke Hijmans, 'The European Data Protection Supervisor: The Institutions of the EC Controlled by an Independent Authority', *CMLRev.* 43 (2006) 1313–42.

Next to these general provisions on data protection, many policy-specific provisions on use of data also contain elements of data protection. These have been created in the EU in particular in areas with especially intensive use of data. This applies, for example, to the field of asylum and immigration through rules on the EURODAC database within the implementational framework of the Dublin Convention,[67] to investigations carried out by the anti-fraud unit OLAF[68] concerning EU statistics,[69] to the supervision of EU agricultural aid schemes,[70] and to the framework of the 'Naples II' Convention on cooperation between customs administrations.[71]

Problems for data protection often arise from the architecture of large-scale IT systems which have emerged in recent years and which have been aimed mostly at enabling cooperation in the joint administrative space. Although each database has a different purpose, these systems share common features. One is that they often contain large volumes of data about many individuals. They are also often similar in structure, consisting both of, on the one hand, national organizations and, on the other hand, a central European unit. This necessitates cooperation among data protection supervisors from both the EU and the Member States. The just mentioned EURODAC system exemplifies this, under which responsibilities for data protection supervision are shared between the EDPS and Member State supervisors.[72] A coordinated approach is essential, supervision depending for its effectiveness on such collaboration.[73]

---

[67] See Arts 4–7 and 15 of Council Regulation (EC) 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2000 L 316/1. The Dublin Convention has been replaced by Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2003 L 50/1.

[68] See eg Art 8 of Regulation (EC) 1073/1999 of the European Parliament and of the Council of 25 May 1999 concerning investigations conducted by the European Anti-Fraud Office (OLAF), OJ 1999 L 136/1.

[69] Arts 13–18 of Council Regulation (EC) 322/97 of 17 February 1997 on Community Statistics, OJ 1997 L 52/1.

[70] Art 13 of Council Regulation (EC) No 73/2009 of 19 January 2009 establishing common rules for direct support schemes for farmers under the common agricultural policy and establishing certain support schemes for farmers, amending Regulations (EC) No 1290/2005, (EC) No 247/2006, (EC) No 378/2007 and repealing Regulation (EC) No 1782/2003, OJ 2009 L 30/16.

[71] Council Act 98/C 24/01 of 18 December 1997 drawing up, on the basis of Article K3 of the Treaty on European Union, the Convention on mutual assistance and cooperation between customs administrations, OJ 1998 C 24/1.

[72] EURODAC is a large-scale IT system which contains digital fingerprints of asylum seekers. It consists of national units, subject to national law, and a central unit, regulated by EU law (Regulation (EC) 45/2001). See Regulation (EC) 2725/2000 (the latter convention has been Replaced by Council Regulation (EC) No 343/2003 of 18 February 2003 establishing the criteria and mechanisms for determining the Member State responsible for examining an asylum application lodged in one of the Member States by a third-country national, OJ 2003 L

The core of the protection of individuals is found in the possibility of establishing quickly and surely which data on an individual are held, and in remedies such as rights of correction or amendment and of claims to damages to make good individual suffering. Currently, the transparency in the use of, and responsibility for, data in the European administrative system is seriously hampered by the fragmentation of competences between the Member State and European levels coupled with the existence of different standards and responsibilities within the continuing elements of the EU pillar structure. Also, there is no generally accepted standard of data protection. Across the diverse regulatory instruments formulations of the protection vary, sometimes substantially, making it difficult to identify a common thread in regard to the enforceable rights. Such variation is all the more problematic, given the sharing of data between authorities and its use for the achievement of diverse policy goals governed by differing legal rules.

In view of this, the case law of the CJEU has made a big contribution to the interpretation of the provisions on privacy and data protection placing great importance on data protection rights – both in absolute terms and in balancing data protection rights with privacy protection.
The high level of data protection requirements is visible especially with respect to storage of data by private actors for possible law enforcement purposes and with regard to international transfers of data in cases such as *Digital Rights Ireland* [74] and *Schrems.*[75]

Digital Rights Ireland concerned the processing of data through the obligation of retention of telecom connection data by telecom operators in the EU.

This was regarded by the CJEU as a serious limitation of the right to privacy and the protection of personal data protection since to 'establish the existence of an interference

---

50/1); Council Regulation (EC) 407/2002 of 28 February 2002 laying down certain rules to implement Regulation (EC) 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2002 L 62/1; Commission Communication regarding the implementation of Council Regulation (EC) 2725/2000 'EURODAC', OJ 2003 C 5/1.

[73] The EDPS organizes, therefore, biannual coordination meetings. Since January 2004, the EDPS has ensured the supervision of the central unit of EURODAC. An essential aspect of this supervision is the cooperation with national supervisory authorities and the drawing up of recommendations for common solutions to existing problems, often adding to conflicts of responsibility and an unintelligible system of protection of rights to individuals, see: <http://www.edps.europa.eu>.

[74] Joined Cases C-293/12 ad C-594/12 *Digital Rights Ireland* of 8 April 2014.

[75] C-362/14 *Schrems v DPC* of 6 Oct 2015.

with the fundamental right to privacy, it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way.'[76] Additionally, the potential 'access of the competent national authorities to the data constitutes a further interference with that fundamental right'.[77] The interference was particularly serious since, despite not containing the content of the communication, the data retained under the law

> 'taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.''[78]

In reviewing whether such limitation were justified by the law, the Court found that even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference with those rights, this interference is 'not such as to adversely affect the essence of those rights given that, as follows from Article 1(2) of the directive, the directive does not permit the acquisition of knowledge of the content of the electronic communications as such.'[79]

However, the Court of Justice in the first ever finding of violation of the essence of a fundamental right in an EU legal act, found in *Schrems*[80] with reference to *Digital Rights Ireland,* that it is impossible to consider purpose limitation to be complied with where legislation

> 'authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the EU to the US without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use for purposes which are

[76] Joined Cases C-293/12 ad C-594/12 *Digital Rights Ireland* of 8 April 2014, para 33.
[77] Joined Cases C-293/12 ad C-594/12 *Digital Rights Ireland* of 8 April 2014, para 35.
[78] Joined Cases C-293/12 ad C-594/12 *Digital Rights Ireland* of 8 April 2014, para 27.
[79] Joined Cases C-293/12 ad C-594/12 *Digital Rights Ireland* of 8 April 2014, para 39.
[80] C-362/14 *Schrems v DPC* of 6 Oct 2015.

> specific, strictly restricted and capable of justifying the interference which both access to that data and its use entail'.[81]

The Court continunes in *Schrems* where public authorities have 'access on a generalised basis to the content of electronic communications' this compromises 'the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter'.

Only where the essence of a right is guaranteed can there be reivew of justification of limitations under the criteria of Art. 52(1) CFR under which limitations have to be proportionate. With regards to limitations the rights to privacy and protection of personal data it is well accepted that an analogy from ECHR Convention 108 is to be undertaken under which data revealing race, political orientation, beliefs, sexual orientation and sex-life are particularly sensitive. Although this approach is not explicitly mentioned in Art 8 CFR, but are factored into the possibilities of limitation of a right under Art. 8 CFR and the requirements of proportionality.

Directive 95/46 is applicable not to matters of national security in the Member State exclusive completence, much as Regulation 2016/679 (on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) excludes public law enforcement activity.

However, the case law of the ECtHR is applicable to exactly that field of law and the recent interpretation of Article 8 ECHR with respect to public surveillance legislation is entirely in line with the case law of the CJEU making the criteria for review by the CJEU higly compatible with that of the ECtHR. A detailed case of review of EU Member States surveillance systems has for example been undertaken in *Szabo and Vissy v Hungary*.[82] There, the Strasbourg Human Rights court held that the 'threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives' requires that the

> 'the potential of cutting-edge surveillance technologies to invade citizens' privacy, the Court considers that the requirement "necessary in a democratic society" must be

[81] C-362/14 *Schrems v DPC* of 6 Oct 2015, para 93.
[82] ECtHR of 12 January 2016, *SZABÓ AND VISSY v. HUNGARY (Application no. 37138/14).*

> interpreted in this context as requiring "strict necessity"… . In the Court's view, any measure of secret surveillance which does not correspond to these criteria will be prone to abuse by the authorities with formidable technologies at their disposal. '[83]

Criteria applied by the Court include such factors as the duration of surveillance, the amount and type of data collected and the possibilities of judicial review (i.e. this criteria can also be used not as stand-alone right like in *Schrems*, but as part of the proportionality review of limitations).[84] A central issue common to both the stage of authorisation of surveillance measures and the one of their application is the absence of judicial supervision. » Political supervision is not sufficient.

One factor to take into account with respect to this distribution of powers between CJEU and ECtHR review is that as far as the EU agencies of the Common Foreign and Security Policy (CFSP) (former EU Second Pillar) are concerned, there is no harmonized standard or general framework governing data processing.[85] Article 39 TEU does impose independent control of data processing in the CFSP, but the Council will retain its exclusive right to adopt rules regulating data processing and protection in this field.

With regard to the legal framework of the field of Police and Judicial Cooperation in Criminal Matters (PJCC) (former EU Third Pillar), a new 2016 Directive addresses Member State activitiy in the area of enforcement of criminal law.[86] Often, however, data collection and use does take place in that context, involving heavy reliance on exchange of information among organizations. Both Europol and Eurojust were instituted having an internal data protection officer and an independent 'joint supervisory body' (JSB), composed of representatives of national data protection authorities, charged with the duty of supervising compliance with data protection rules.[87] The JSBs are charged with

---

[83] ECtHR of 12 January 2016, *SZABÓ AND VISSY v. HUNGARY (Application no. 37138/14),* para 73.
[84] ECtHR of 12 January 2016, *SZABÓ AND VISSY v. HUNGARY (Application no. 37138/14),* para 75.
[85] Alfonso Scirocco, 'The Lisbon Treaty and the Protection of Personal Data in the European Union' [2008] European Data Protection Review, No 5 <http://www.dataprotectionreview.eu>.
[86] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ 2016 L 119/89.
[87] See for the details on the JSB of Eurojust, Arts 17, 19, and 23 of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (Eurojust), OJ 2002 L 63/1

reviewing those agencies' activities in regard to potential violation of individuals' rights through the storage, processing, and utilization of data. They do so through inspections, examining and commenting on the opening of specific analysis files, and monitoring the permissibility of the transmission of data, as well as the application of rules governing the transmission of personal data to third party bodies and non-Member States.[88]

4. Relation between openness and data protection

Transparency and data protection rights can collide,[89] an example of the conflict of fundamental rights for which balancing procedures have been developed.[90] Limitations on privacy rights are, for example, explicitly recognized in Article 8 ECHR, allowing these to the extent 'necessary in a democratic society'. Freedom of information is a fundamental principle of an open and transparent society, the basic of a democratic system under the rule of law. Further, the inherent complexity of the European Union requires special efforts to anchor and extend transparency in order to achieve a democratically accountable political and administrative system. On the other hand, the complexity of data-sharing structures in the EU's integrated administrative system also requires extra vigilance as regards data protection. Therefore, where a conflict between data protection and freedom of information arises, these rights must be carefully balanced in order to maximize the potential of each in its correct role.

---

and the Act of the Joint Supervisory Body of Eurojust of 2 March 2004 laying down its rules of procedure, OJ 2004 C 86/1. For details of the Europol JSB, see the Council Decision of 6 April 2009 establishing the European Police Office, OJ 2009, L121/49. International data exchange is authorized under Council Decision of 27 March 2000 authorising the Director of Europol to enter into negotiations on agreements with third States and non-EU bodies, OJ 2000 C 106/1.

[88] See: <http://europoljsb.consilium.europa.eu/default.asp?lang=EN>.

[89] See Case T-194/04 *Bavarian Lager v Commission* [2007] ECR II-4523 (Appeal C-28/08 P) in which the Commission had rejected the applicant's request to access to information. In support of its refusal it invoked the need to protect personal data of the persons present at the meeting, as well as a potential risk to the Commission's ability to carry out investigations in such cases if the identity of persons giving information to the Commission were to be disclosed. Sharpston AG, in her opinion of 15 October 2009 on Case C-28/08 P *Commission v Bavarian Lager*, ECR nyr, judgment of 29 June 2010, paras 156–166, gives an excellent overview of distinguishing criteria. The CJ upon review in Case 28/08 P *Commission v Bavarian Lager* [2010] ECR I-nyr, although setting aside the judgment of the General Court, confirmed that the contested Commission decision not to disclose the names sought neither infringed Regulation 1049/2001 nor 45/2001 (paras 69–73). See also now the Grand Chamber in Case C-92/09 Schecke [2010] ECR I-nyr of 9 November 2010.

[90] See with further examples, Timothy Pitt-Payne, 'Privacy versus Freedom of Information: Is there a Conflict?', *EHRLRev.* (2003) Supplement 108–11.

The European Ombudsman (EO)[91] has in the past highlighted the dangers of potential misuse of data protection provisions so as to limit public access to documents and to contradict the principle of openness. The effective implementation of the public right to access to documents, he argued, 'could be undermined if the staff responsible for releasing documents work in fear that they may be punished for violation of data protection rules merely because a document contains a [person's] name'.[92] He pointed out that the right of access to documents is a fundamental procedural right, generally not allowing for a discretionary decision by the administrative body concerned.[93] One should add, though, that despite its obvious correctness, this proposition needs to be seen in the context of the possible conflict of fundamental rights.

The solution of such a potential conflict is closely linked to the application of the principle of proportionality. Every EU measure must be proportionate. This is directly connected with the overarching principle of the public administration, namely, that it is to serve those affected by it through open decision-making procedures, so that any citizen can carry out 'genuine and efficient monitoring of the exercise of the powers vested in the Community institutions'.[94] As already discussed above, the central norm for balancing the right of public access to documents, on one hand, with the right to privacy and protection of individual data, on the other, is currently Article 4(1)(b) of Regulation 1049/2001

[91] With further explanations to the role and the procedures of the EO, see below Chapter 29.

[92] European Ombudsman Letter of 14 November 2001, at: <http://ombudsman.europa.eu/letters/en/20011114–1.htm>.

[93] According to the Ombudsman, 'there is nothing in Article 286 EC or the data protection Directive to suggest that data protection rules should be applied as a general principle of confidentiality in public administration, so as to require a balancing exercise whenever a document contains a name' (European Ombudsman Letter of 14 November 2001, at <http://ombudsman.europa.eu/letters/en/20011114–1.htm>). The dangers, to which the EO points, are real. If the fact that individuals enter into the public domain to work for institutions, or to represent their interests, could lead to the automatic right of institutions and bodies of the EU to refuse access to documents, the data protection argument could then easily be distorted to maintain secretive policies. This would be especially dangerous in the European context where there are complex public procedures and institutional arrangements, involving an integrated administration relying on composite mechanisms with Member State and EU participation. Transparency is the best tool in the fight against the possibilities of nepotism and the dangers of corruption. The examples cited by the EO are informative. They include, eg, the EP's refusal to allow the publication of names of successful candidates in open competitions for its jobs and to change the institutional practice to promise confidentiality to them. They also include the publication of names of individuals working for the institution, and of the MEPs. Another matter which the EO criticizes is the Commission's practice of maintaining the secrecy of procedures under Art 258 TFEU (Art 226 EC), through which the Commission controls Member States' compliance with EC law. As the EO correctly points out, there is no fundamental right to anonymity when participating in public affairs. See with greater detail, European Ombudsman Letter of 25 September 2002, on the misuse of data protection rules in the European Union, at: <http://ombudsman.europa.eu/letters/en/20020925-1.htm>.

[94] Case T-92/98 *Interporc v Commission (Interporc II)* [1999] ECR II-3521, para 39.

which sets out the exceptions to the right of access. Even though under that provision the protection of personal data can make a refusal of access mandatory, like every public decision, such a decision to refuse must itself be proportionate, and in doing so balance the right of individuals to openness and access to documents with the individual right of data protection. This requires taking the following three basic aspects into account.[95] First, the 'privacy and integrity' of the data subject which may be at stake by publication of the document must be respected.[96] Secondly, the decision must consider whether public access would in fact 'undermine' the protection of such privacy rights, that is, substantially affect the data subject.[97] Finally, the potential harm to a person's integrity and privacy needs to be evaluated 'in accordance with Community legislation regarding the protection of personal data'. This will require attention to whether possible compromise solutions including partial access to documents or access subject to such deletion of the references as are necessary to protect private information will resolve the conflict. It is for an applicant seeking access to data to provide 'any express and legitimate justification or any convincing argument in order to demonstrate the necessity for those personal data to be transferred' so as to allow the authority to weigh up data protection and access to information rights under EU law and to assess 'whether there was any reason to assume that the data subjects' legitimate interests might be prejudiced, as required by the Data Protection Regulation'.[98]

Solving such conflicts has not been facilitated by the existence of two distinct bodies supervising the right to access and the right to privacy, namely the EO and the EDPS. Balancing the rights would be best undertaken by one body, equipped with the

---

[95] For a discussion of these criteria from the point of view of data protection, see European Data Protection Supervisor, Public access to documents and data protection, *Background Paper Series* [2005] No 1, 12–30 (<http://www.edps.europa.eu/EDPSWEB/>).

[96] This will be the case especially with data related to a public function or particularly sensitive date, such as those relating to, eg, personal health or family life.

[97] The notion of undermining the protection of privacy indicates that the negative effect of the disclosure on the private individual would be substantial, in the sense of having not only a marginal effect, but seriously limiting the rights of individuals. This may be the case where access to the information is explicitly targeted at obtaining information about particular private persons, irrespective of whether or not they have public status, functions, and activities.

[98] Case C-28/08 P *Commission v Bavarian Lager* [2010] ECR I-XXX, paras 78–80 in which the Court does no justice to the depth and the breadth of the opinion of Sharpston AG, delivered on 15 October 2009. In her opinion, Sharpston AG skilfully demonstrates how data protection and transparency rules can be reconciled. Unfortunately, the Court allows the Commission, on a rather technical point, to use data privacy rules as a pretext for limiting transparency in administrative procedures.

capabilities of following up maladministration in its various forms. However, it is noteworthy that the powers of the EDPS reach further than those of the EO, despite the fact that the EO is the better known institution having a broader mandate directly supervised by the EP. The EDPS can issue decisions binding on the institution. The EO can, however, only make public recommendations and seek amicable solutions.

5. Conclusions

The question asked at the beginning of this paper was whether the law of information in the EU is developing in the direction of an 'ideal' according to the necssities of a democratic system under the rule of law in the digital age. I argue that the situation in the EU has developed in a way which is not entirely up to those standards.

Although under EU law the protection of personal data is generally ensured to a high degree, especially in the case law of the CJEU, difficulties exist especially with respect to protection of data in view of public collection by a diverse set of information systems and by a diversity of EU bodies and associated data protection responsibilities. This makes it particularly difficult for individuals to assess responsibilities and to seek remedies. Since data protection is highly linked to transparency in the sense of transparency of responsibilities of data collection as well as rights of access to know what data has been stored and used, clearly defined responsibilities and unified responsibilities of control and supervision are necessary.

All in all, there is a very unhealthy multiplication of legal rules on data protection, and of data protection authorities, each applying different rules to specific sub-sectors of the EU. Coordination appears to be difficult. This is worrisome, especially since cooperative activities in the administrations of customs, policing, and other aspects of law enforcement often touch areas where, due to the sensitivity of the information involved and the dangers of violations of individual rights arising from its uncontrolled use, data protection is most seriously and urgently required. The dangers which arise here from data handling, exchange, and use, as outlined above, especially those resulting from the combination of eventually erroneous information with other data and the subsequent data

exchanged can be very significant.[99] Effective protection of individuals also requires the possibility of establishing quickly and surely which data on an individual are held, as well as the availability of remedies such as rights of correction or amendment and of claims to damages to make good individual suffering. Currently, the transparency in the use of, and responsibility for, data in the European administrative system is seriously hampered by the fragmentation of competences between the Member State and European levels coupled with the existence of different standards and responsibilities within the continuing elements of the EU pillar structure. Also, there is no generally accepted standard of data protection. Across the diverse regulatory instruments formulations of the protection vary, sometimes substantially, making it difficult to identify a common thread in regard to the enforceable rights. Such variation is all the more problematic, given the sharing of data between authorities and its use for the achievement of diverse policy goals governed by differing legal rules.

Remedies for these weaknesses can, however, be identified given that many of the problems associated with privacy and data protection are common to different policy areas.[100] The first such problem is the difficulty individuals face in discovering what information about them has in fact been collected and stored, in which contexts, and in which registers or databases. Knowledge of this is essential and should be provided, within the limits of ongoing investigations.[101] Such a right of access, given the distribution of data throughout the diverse European databases and, according to the technical setup, 28 national databases mirroring information and adding as well as further computing such information, needs to be established through a central unit on the EU level.

This shows that rules on access to information are not only also pre-conditions for effective enforcement of individual rights on privacy and data protection, but, as was well understood in Sweden some 250 years ago, rights of access to publically held information

[99] For details see Spiros Simitis (ed), *Bundesdatenschutzgesetz Kommentar* (Baden-Baden: Nomos, 2006) introduction, 65–6, paras 9–12.

[100] See for an excellent overview and critique, Steve Peers, 'Human Rights and the Third Pillar' in Philip Alston (ed), *The EU and Human Rights* (Oxford: Oxford University Press, 1999) 167–87 at 180.

[101] This principle has been established as the basic level by the ECHR in *Leander v Sweden* ECHR (1987) Series A, No 116, 48.

are also more generally, a pre-condition to an open and democratic society under the rule of law.

However, on the EU level, despite promising developments in the past 15 years ago with the adoption of Regulation 1049/2001 and the adoption of the Aarhus Regulation in the field of environmental information, much damage has been done by the rolling back of rights of access to documents. Such rolling back has been undertaken by a highly restrictive interpretation of the existing rights by the CJEU, especially with respect to documents held regarding administrative procedures. Also, the balancing between privacy and transparency has been undertaken allowing administrations to hide behind privacy considerations in order to circumvent basic requirements of transparency as the case *Bavarian Lager* aptly illustrates. Such case law development leaves the EU to slide to a situation which dangerously restricted transparency rules.

I tried to illustrate the regulatory choices with outlining a spectrum at the beginning of this talk, according to which the ideal of a democractic society under the rule of law is that public information and affairs are public whilst private matters are protected as private can be constrasted with the 'ideal' of a totalitarian system under which all public matters are secret whilst the public has full access to all matters private. When looking at where the EU stands on this spectrum, it would appear that there is great concern form maintinaing privacy, although the approach is often flawed by a lack of a coherent overarching structure to do so. The concept of transparency and access to documents has become less and less protected with broad and sweeping exceptions being introduced in disrespect of the spirit of the EU law in place. Therefore, although the EU is not in danger of moving into the spectrum of the totalitarian ideal, much effort needs to be undertaken, to live up to the necessities of an open system under the rule of law.