Privacy and Data Protection in the UK and in the EU: A Long History of Divergence Even During EU Membership-Brexit Should Not Bring a Divorce with the EU Privacy Regulatory Regime so as to Protect Trade and Human Rights in the UK

MARIOS KOUTSIAS*

Abstract

The article examines data protection in the UK and in the EU and it argues that the UK should remain compliant with the EU data protection regulatory regime after Brexit. This is imperative for two reasons; to consolidate trade with the EU which evolves in the challenging environment of Brexit but also to maintain a high level of human rights' protection. To that end, the article examines the legislative, political and cultural background of privacy in the EU and in the UK. It will then focus on data protection which is merely an aspect of the umbrella right of privacy. The English legal traditions on privacy diverged from the respective European ones. They came to somehow converge only with the passing of the Human Rights Act in 1998 and the EU Data Protection Directive of 1995. The UK was uneasy with the regulation of privacy and data protection even throughout its EU membership. Brexit which entails a rupture with the EU legal order may therefore bring a lesser protection of privacy and personal data in the post-Brexit English legal order especially since the UK is now contemplating withdrawal from the entire European institutional network of human rights protection. That will impact upon the status of the right to data protection too which is an aspect of the right to privacy and it is instrumental for maintaining trade with the EU. This is because article 45 GDPR requires an adequate level of protection of the personal data of EU citizens in order to allow their transfer to a third country; this is effectively a pre-requisite to trade. If the post-Brexit UK reverts to lesser standards of protection that will entail both an erosion of human rights' protection in the country as well as significant economic damage.

Keywords

Data protection, privacy, EU Law, Brexit, GDPR, UK GDPR, comparative law, business law, human rights law, internet law.

* Dr Marios Koutsias, Senior Lecturer in European Union Law and Company Law, Law School, University of Essex, UK.

Koutsias, Marios, 'Privacy and Data Protection in the UK and in the EU: A Long History of Divergence Even During EU Membership-Brexit Should Not Bring a Divorce with the EU Privacy Regulatory Regime so as to Protect Trade and Human Rights in the UK'. *European Business Law Review* 36, no. 1 (2025): 103-132.

Introduction

The article examines data protection in the UK and in the EU and it argues that the UK should remain compliant with the EU data protection regulatory regime after Brexit. The article argues that this is imperative for two reasons; to consolidate trade with the EU which evolves in the challenging environment of Brexit but also to maintain a high level of human rights' protection. To that end, the article will examine the legislative, political and cultural background of privacy in the EU and in the UK. It will then focus on data protection which is merely an aspect of the umbrella right of privacy. This article explains that privacy as a concept and consequently as a right has its roots in ancient times. Data protection on the other hand was born as a result of the technological developments of the 20th century. Therefore, the analysis of the right to privacy will shed light on the genesis and on the evolution of the separate right of data protection too.

The article looks at the historical, political, cultural and legal roots of privacy in order to fully comprehend the place that it has in the contemporary EU legal order. It compares and contrasts that with the respective evolution of the right to privacy in England. Then the article looks at data protection; it argues that since data protection is only an aspect of the mother right of privacy, it naturally presents the characteristics and challenges of its mother right. Therefore, to understand data protection, it is necessary to understand privacy.

Privacy is one of those rights whose nature, essence and definition were heavily affected by the cultural context within which they evolved. Different perceptions of what should be kept private and what should be in the public domain depend very much on the dominant philosophical, societal, cultural and at the end legal principles in any society. Therefore, different cultural approaches to privacy entail different laws on privacy and consequently of data protection. The establishment of an independent right of privacy in the UK was only a by-product of its EU membership. In this context it is easy to discern the challenges that Brexit entails on the continuous recognition of such right by the English legal order.

The conceptual background which forms the substance of privacy and therefore of its distinctive aspect too of data protection will be examined. Privacy will be defined albeit not in a single and homogeneous way simply because literature has not converged into a single definition of the term; this is reflective of the divergent cultural backgrounds and values that shaped the modern notion of privacy. The evolution of privacy within the European historical, philosophical, legal and theological landscape is explained in detail. Privacy as a concept may be as ancient as the roots of what we can define as European culture, but it is still hard to converge into a single definition due to its dependence on distinctive cultural perceptions.

The English legal traditions on privacy diverged from the respective European ones. They came to somehow converge only with the passing of the Human Rights Act in 1998 and the EU Data Protection Directive of 1995.[1] The UK was uneasy with

[1] 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.

the regulation of privacy and data protection even throughout its EU membership. Brexit which entails a rupture with the EU legal order may therefore bring a lesser protection of privacy and personal data in the post-Brexit English legal order especially since the UK is now contemplating withdrawal from the entire European institutional network of human rights protection. Since the ECHR provides for the right to privacy as a human right, any exit from the Convention will undermine the status of privacy within the English legal order. That will impact upon the status of the right to data protection too which is an aspect of the right to privacy and it is instrumental for maintaining trade with the EU. This is because article 45 GDPR[2] requires an adequate level of protection of the personal data of EU citizens in order to allow their transfer to a third country; this is effectively a pre-requisite to trade. Therefore, maintaining the current level of data protection in the UK is instrumental for maintaining trade with the EU; this is vital for the UK economy. If the post-Brexit UK reverts to lesser standards of protection that will entail both an erosion of human rights' protection in the country as well as significant economic damage. The article will argue against that.

The Evolution of Privacy in Europe and the Birth of Data Protection

In Europe privacy is a fundamental right, yet it is not an absolute one.[3] The actual existence of "privacy" as an independent concept can be traced back into classical Greece and Rome. Culture and privacy were closely linked in ancient times too, hence a lack of a common definition of privacy even then. In Ancient Greece "public" was "demos" which means the people. In a society based on direct democracy and active participation in public life any withdrawal from it was viewed negatively. The word for private was "idios". The term had negative connotations reflected in the fact that the word constitutes the linguistic origins "from which comes the English word idiot".[4] "Idios" or "idiotis" in modern Greek was the person who chose to abstain from public affairs; "idiotis" was an apolitical being who expressed the desire to be left alone.[5] The participation in public life and affairs encouraged excellence spurred by social scrutiny while isolation into the private sphere brough selfishness and swallow attitudes.[6] Looking at Aristotle we do discern the separation between the public and private spheres of life.[7] The public sphere was the "polis" (in modern Greek the "city") where politics (deriving from "polis") took place. Men are political animals

---

[2] General Data Protection Regulation, Regulation 2016/679. See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679.

[3] David Banisar, Simon Davies, *Global Trends In Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments* 18 The John Marshall Journal of Computer and Information Law 5 (1999).

[4] Moore JR Barrington, *Privacy, Studies in Social and Cultural History*, 82 (New York, M.E. Sharp Inc 1984).

[5] Above, 118.

[6] C Velecky Lubor in John B. Young, *Privacy*, 16 (New York, John Wiley & Sons, 1978).

[7] See Judith Wagner DeCew, *In Pursuit of Privacy*, 10 (Ithaca, Cornell University Press, 1997).

and therefore expected to participate in politics. But, the sphere of the polis, which was common to the free citizens, was strictly separated from the sphere of home "oikos"; in the sphere of the "oikos", each individual is in his own realm.[8]

The Romans defined privacy similarly to Ancient Greeks. The Latin roots of the term privacy are "privatus" and "privare". The former meaning "withdrawn from public life" and the latter "to bereave or deprive".[9] In the Roman context, retreat to a private sphere can provide a temporary refuge from the demands of public life".[10] Interestingly enough, the German word privat, which was borrowed from the Latin privatus, the English "private" and the French privé all mean "not holding public office or official position".[11] Although elements of privacy can be traced back in the cultures which provided the pillars of Western thought and culture, its modern form was defined by the advent of human rights as a pillar of a democratic society and the need to consolidate free trade by allowing the free movement of personal data if certain fixed legal requirements are met. In this context the right to privacy as well as data protection are now protected by law. In today's western liberal tradition, the right to privacy arises from the relationship between the "individual with society and the nation state".[12] This is because the European legal culture now concedes that in a way "all human rights are aspects of the right to privacy".[13]

This is due to the World War II. In the 1960s the government of the German federal state Hesse, announced plans to collect the personal data of its citizens to plan its policies effectively bringing memories of the vile Nazi policies of population control and of extensive surveillance.[14] The so-called Hollerith machines contributed to the "vast data processing apparatus of Nazi Germany" playing no small part to the Holocaust.[15] This was the context within which data protection was born as a means to protect the right to privacy. The first Data Protection legislation in the world was passed and data protection became a distinctive subset of privacy. It also led Europe to establish its approach to data protection opting for state regulation of the field. Sweden was the second country to follow as early as 1973. France and Germany

---

[8] Jiirgen Habermas, *The Structural Transformation of the Public Sphere*, page 3 (Cambridge, Massachusetts, The MIT Press, 1993), at: https://courses.ischool.berkeley.edu/i218/s15/Habermas_STBPS_I.Intro.pdf.

[9] Paul De Hert in C. Nicoll, J.E.J Prins, M.J.M. van Dallen*, Digital Anonymity and the Law, Tensions and Dimenions*, 56 (The Hague, T.M.C. Asser Press, 2003).

[10] Above.

[11] Jiirgen Habermas, *The Structural Transformation of the Public Sphere*, page 11 (Cambridge, Massachusetts, The MIT Press 1993), at: https://courses.ischool.berkeley.edu/i218/s15/Habermas_STBPS_I.Intro.pdf.

[12] Bruno Zeller, Leon Trakman, Robert Walters, Sinta Dewl Rosadi, *The Right to be Forgotten – The EU and Asia Pacific Experience* 1 European Human Rights Law Review 24 (2019).

[13] David Banisar, Simon Davies, *Global Trends In Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments* 18 The John Marshall Journal of Computer and Information Law 4 (1999).

[14] Tracie Loring B., *An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States* 37 Texas International Law Journal 423 (2002).

[15] Jef Ausloos, *The Right to Erasure in EU Data Protection Laws*, 39, (Oxford, OUP, 2020).

passed their general data protection laws by the end of that decade. In the fifties and sixties, the fears for privacy concerned mainly the government activities and policies as it was this informational aspect of privacy affected by technology the most in the 1960s.[16] The citizens identified a threat to their privacy stemming from state activities. Now, they resort to the state to alleviate fears of privacy invasion by private companies or individuals too. The shift in the trend has been radical and has prompted the EU to adopt the European Directive on Data Protection[17] that has changed the regulation of data protection for good. The latter was therefore historically based on substantive values such as dignity, autonomy, self-development and self-determination[18] and became the central field for the "development of privacy law and policy".[19]

The Landmark Directive 95/46 on Data Protection and its Links with the Internal Market

The truth is that "historically the European Commission has not concerned itself with data protection".[20] The relevant legislative measure was introduced in the framework of its internal market programme, which serves as the clearest indication of the dual objective of the Commission. Both goals had to be equally and effectively served. An effective protection of a fundamental right of the European citizens and the facilitation of trans-border flow of personal data that constitutes the basis for trade in the single market. The directive was passed under the umbrella provision of article 100a of the EC Treaty,[21] which allows the promotion of measures for the approximation of laws regarding the internal market. In 1989 the Commission will taste the sort of problems that could have rocked the single market if common action was not taken. In the *Fiat*[22] case, CNIL – the French data protection authority – intervened in a transfer of employees' data from the French to the Italian branches of the company because Italy lacked data protection legislation.[23] This signalled that cumbersome procedures and negotiations will need to take place within the internal market even for basic cross-border business activities. In December 1993 the European Commission of

---

[16] Adam Warren, *Sources of Literature on Data Protection and Human Rights* 2 The Journal of Information, Law and Technology 3 (2001).

[17] See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046&from=EN.

[18] Marek Szydlo, *The Independence of Data Protection Authorities in the EU Law: Between the Safeguarding of the Fundamental Rights and Ensuring the Integrity of the Internal Market* 42(3) European Law Review 372 (2017).

[19] David Erdos, *European Regulatory Interpretation of the Interface Between Data Protection and Journalistic Freedom: An Incomplete and Imperfect Balancing Act?*, Public Law 633 (2016).

[20] Simon Stokes, *Data Protection* 17 (7) European Intellectual Property Review 215 (1995).

[21] See: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:11992E100A&from=EN.

[22] Commission nationale de l'informatique et des libertas, *lOe rapport d'activite*, 32-34 (1989).

[23] See Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows* 80 Iowa L. Rev. 472 (1994-95).

Jacques Delors published the White Paper on Growth, Competitiveness and Employment[24] and emphasised the importance of "laying the foundations for the information society"[25] because the changes "will also affect citizens".[26] Therefore, "one priority… is to protect privacy".[27] Five member states namely Italy, Greece, Spain, Portugal and Belgium lacked any data protection regulation thus creating economic burden to the French and German firms. Fearing that their firms will shift their data procession business to the member states with no data protection regulations, the French and German governments lobbied for EU-wide action[28] and pushed for EU-wide legislation "hoping to level their playing field for their national firms within the single market".[29] Divergent standards of data protection within the EU undermined the free movement of personal data;[30] therefore, the very operation of the single market. Consolidating a single market within which personal data flows on common legislative standards[31] was instrumental. The free movement of services, goods and companies – the pillars of the single market – are underlined by the free flow of personal data. In the 1990s it was yet another fundamental aspect of the internal market that emerged in conjunction with data protection; the free movement of people. The EU was moving towards the removal of border controls and checks for EU citizens within the internal market. To that end it signed and gradually implemented the Schengen Agreement whose operation was dependent upon the Schengen Information System which was essentially a large border control database which collected personal data of EU travellers. For the system to work all member states of the EU which aimed at integrating to that system needed data protection rules in place; otherwise, the system would evolve into a major threat to EU citizens' privacy. In this context data protection was linked to yet another fundamental freedom of the internal market. Commissioner Martin Bangemann concluded that "data privacy was central to the internal market and for guaranteeing the free movement of individuals within the community".[32] At the end it was clear, that with no data protection, there can be no internal market. At that point data protection was not "a right in itself"[33] but rather a mechanism to ensure the free movement of data within the internal market. Therefore, the protection

---

[24] White Paper on Growth, Competitiveness and Employment, *The Challenges and Ways Forward into the 21st Century*, COM (93) 700 final, Brussels (5 December 1993), see: http://www.gencat.es/csi/pdf/eng/soc_info/basic/WP_growth.pdf.

[25] Ibid at 16.

[26] Ibid at 17.

[27] Ibid at 19.

[28] Abraham Newman, *Protectors of Privacy*, 11 (Ithaca, Cornell University Press 2008).

[29] Abraham Newman, *Protectors of Privacy*, 7 (Ithaca, Cornell University Press 2008).

[30] Christopher Rees, Kate Brimsted, *The Twelve Stages of Data Protection, IT Law Today*, 24 (2002).

[31] Christina Ramberg Hultmark, *The E-Commerce Directive and Formation of a Contract in a Comparative Perspective* 26 European Law Review 429 (2001).

[32] Abraham Newman, *Protectors of Privacy*, 90 (Ithaca, Cornell University Press, 2008).

[33] Dennis Kelleher, Karen Murray, *EU Data Protection Law*, 4 (London, Bloomsbury Professional, 2021).

of data assumed a dual "normative rationale";[34] the protection of a fundamental right and the smooth operation of the internal market. The combination of a "market integration rationale with a fundamental right logic is remarkable against the backdrop of the history of European economic integration"[35] which has favoured economic integration over fundamental rights. After all the EU began its journey as the European Economic Community.

Looking at the neo-functionalist theories which see the commission as seizing opportunities to expand its supranational jurisdiction to new areas one can also argue that the commission was very eager to promote this agenda not only for the aforementioned reasons but also because it discerned a clear chance to expand its supranational powers[36] and forge its authority firmly into a new emerging but obviously very significant new field; the digital economy.

The Legal Basis for Protecting Personal Data in the EU

An additional legal basis for its initiatives was Article 8 of the European Convention for the protection of Human Rights and Fundamental Freedoms. Article 8 ECHR extends to fields where the EU lacks the legislative competence to act such as aspects of family law, criminal or civil law which form part of the national legal orders, but it still functioned as the basis for the EU to regulate the protection of privacy and then to extend its ambit into the protection of personal data as a subset of privacy. The Convention rights are now part of general principles of EU law.[37] The new Article 6TEU[38] safeguards rights enshrined in the ECHR. The new article 16TFEU,[39] and article 8 of the Charter of Fundamental Rights[40] now constitute concrete legal basis for the protection of data at the EU level; both part of the "constitution order" of the EU. The directive may have been a compromise between the protection of general principles of law with overriding constitutional importance within the legal order of member states[41] and the smooth operation of the common market but data protection

---

[34] Svetlana Yakovleva, *Should Fundamental Rights to Privacy and Data Protection Be a Part of the EU's International Trade 'Deals'?* 17 World Trade Review 477-508 (2018), at SSRN: https://ssrn.com/abstract=3245982.

[35] Thomas Streinz, *The Evolution Of European Data La*w, 14 (2021). Accessed at the SSRN network at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3762971.

[36] See: Dorothee Heisenberg, *Negotiating Privacy: The EU, the US and Personal Data Protection* (Lynne Rienner Publishers, 2005).

[37] Rosemary Jay, Angus Hamilton, *Data Protection, Law and Practice*, 72 (London, Sweet & Maxwell, 2003).

[38] See the Article at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A12008M006.

[39] See the Article at: https://www.legislation.gov.uk/eut/teec/article/16.

[40] See the Article at: https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data.

[41] Korff Douwe, *EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws*, 6 (Cambridge, September 2002). See: https://gegevensbeschermingsrecht.nl/onewebmedia/douwe.pdf.

is now an independent right of its own in the EU legal order. In *Rundfunk*[42] the CJEU clarified that the directive must "necessarily be interpreted in light of fundamental freedoms". It is interesting to see that article 8 of the Charter is actually based on the directive. According to the explanatory memorandum to article 8 of the Charter "article 8 has been based on Article 286 of the (then) Treaty and Directive 95/46/EC".[43] Rights, even "when they are new rights are rarely taken from a vacuum".[44] Therefore, it was the directive which created a pan-European right to data protection and became the legal basis for significant texts like the Charter which later on became part of the Treaty. The directive aimed at fostering harmonisation of national legislation in order to remove the legal obstacles that impact upon the free movement rules.[45] In its heart laid the principle that an organisation cannot do anything with the "personal data of an individual unless it is permitted by the law".[46] In any case, the incorporation of the Charter into the treaty is important as now privacy and data protection are subject to article 48TEU[47] which requires unanimity for their reform. In addition to that the EU must secure compliance with the Charter in all areas of legislative drafting.[48] But this is the first time that a community measure aims at protecting human rights within the context of the internal market.[49] The aim was that if all member states adhere to the minimum standard of protection, there should be free movement of personal data within the EU.[50]

The effect of the directive and later on of the Charter on the national legal orders of the member states was substantial enough to trigger constitutional reform; Sweden, the Netherlands, Spain, Poland, Hungary[51] but also Greece and Belgium added the right to data protection to their constitutions.[52] In addition to that, although a general right to privacy preceded the right to data protection, the right to privacy assumed national constitutional status only recently. The first European constitution to include such a right was that of Cyprus in the 1960s, then that of Greece in 1975 and prior to

---

[42] Case C-139/01, *Osterreichischer Rundfunk and Others* [2003] ECR I-4989.

[43] See https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32007X1214(01)&from=EN. Explanations Relating to the Charter, Official Journal of the EU, 14.12.2007. Article 8.

[44] Felix Bieker, *The Right to Data Protection*, 15 (Berlin, Springer, 2022).

[45] Renaud Par De Bottini, *La Directive "Commerce Electronique du 8 Juin 2000*, La Revue du Marche Commun et de l'Union Europeenne 369 (2001).

[46] Sahar Bhaimia, *The GDPR: The Next Generation of EU Data Protection* 18(1) Legal Information Management 22 (2018).

[47] See the Article at: https://www.legislation.gov.uk/eut/teu/article/48.

[48] Marie Pierre Granger, Kristina Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling off the EU Legislator and Teaching a Lesson in Privacy and Data Protection* 39(6) European Law Review 844 (2014).

[49] The European Commission, Final Report by Douwe Korff (contractor), *The Feasibility of a Seamless System of Data Protection Rules for the European Union* (Directorate General XV, Internal Market and Financial Services, 1998, Luxembourg).

[50] David Bainbridge, *Computer Law*, 363 (Fourth Edition, London, Longman, 2000).

[51] Mattoo Aaditya, *International Data Flows and Privacy: The Conflict and Its Resolution* 21(4) Journal of International Economic Law 772 (2018).

[52] Monika Zalnieriute, *An International Constitutional Moment for Data Privacy in the Times of Mass-Surveillance* 23(2) International Journal of Law and IT,106, (2015).

1990 only the Netherlands, Spain and Portugal provided for privacy in their constitutions. Today however, and after the EU law in this field 20 out of 27 member states have a general right of privacy enshrined in their constitutions.[53]

The Other Side of the Channel: The Historical Roots of Privacy in the UK: Property Rights and Liberty – A Very Different Conceptual Framework from the Continental One

Liberty and individual rights stand at the core of the English legal culture. The roots of these doctrines are in Medieval England. England was an agricultural society; trades ancillary to agriculture and rural life were practised locally by individual traders and their families.[54] In the commercial towns both the manufacturers and the merchants "traded under the aegis of the craft guilds".[55] Guilds were organisations that controlled the local market which operated as a monopoly. The guilds would set the regulatory requirements to enter the market themselves along with the conditions that local craftsmen had to fulfil or the standards for the production of local goods. The roots of one of the most fundamental aspects of the English legal culture can be traced at that point: the country's tendency to self-regulate and to avoid state regulation. Personal freedom was defined in this context as "self-help and self-government" as "there were no rights without duties.'[56] All "men are created equal and independent, that from that equal creation they demand rights inherent and inalienable".[57] Individuality and self-regulation enjoy deep roots in English history and privacy could not escape the rule. Matthew Finkin argued that privacy did not come into English until the sixteenth century, a time of increased international trade, economic development and urbanisation.[58] Indeed, the common law became strongly associated with the idea of economic freedom and more generally the subject's liberty from arbitrary action by the Crown.[59] At the end of the 16th century, Shakespeare places Juliet in the seminal balcony scene to ask Romeo who was hiding in the shadows listening to her thoughts: "what man art thou that, thus bescreened in night, So stumblest on my counsel?". Meaning "who are you? Why do you hide in the darkness and listen to my

---

[53] David Erdos, *Comparing Constitutional Privacy and Data Protection Rights within the EU* 47(4) European Law Review 499 (2022).

[54] M.M Postan, *The Medieval Economy and Society* (London, Weidenfeld & Nicolson, and Pelican 1975).

[55] , R.I. Tricker, *The Evolution of the Company, Corporate Governance: Practices, Procedures and Powers in British Companies and their Boards of Directors*, 26 (Gower, Aldershot 1984),.

[56] G.M Trevelyan., *English Social History* (London, Penguin, 1944).

[57] A Macfarlane., *The Origins of English Individualism,* 202 (Oxford, Basil Blackwell, 1978)

[58] Matthew W. Finkin, *Information Technology and Workers' Privacy: A Comparative Study: Part IV: The Comparative Historical and Philosophical Context: Menschenbild: The Conception of the Employee as a Person in Western Law* 23 Comparative Labour Law & Policy Journal 590 (2002).

[59] P.G. Mahoney, *The Common Law and Economic Growth: Hayek Might Be Right* 30 (2) Journal of Legal Studies 508 (2001)

private thoughts?".[60] Despite the fact that they ended up pledging their love for each other, Shakespeare channelled through Juliet the predominant sense even at that time that when someone – Juliet in that case – is "giving voice to her most intimate feelings, that reflects our deepest intuitions about the importance of privacy".[61]

The philosophical foundations of such a debate can be traced before that. Magna Carta, a landmark development in the evolution of English constitutional law and traditions, included a variety of rights with a special emphasis on individual rights. The inclusion of the right to property in the list of fundamental rights and the importance ascribed to personal ownership impacted on many fields of law. Magna Carta placed 'individual liberties above all others except communal rights" [62] a concept adopted by English common law in the thirteenth century. In 1361 the English Justices of the Peace Act provided for the arrest of peeping toms and eavesdroppers. From the beginning the intent to protect an individual from the government was clear: "the poorest man may in his cottage bid defiance to all force of the Crown. It may be frail... the rain may enter; but the King of England cannot enter.[63] This position highlights vividly the prominent position that liberty assumed in the English legal order from a very early point of history. It is translated into the right of any individual to define a space which should be respected by anyone including the highest authority. The definition of privacy in such individualistic terms often results in privacy being undervalued in utilitarian balancing which is the mainstream way that legislators resolve conflicts between interests.[64] Therefore, when privacy conflicts with say the freedom of expression it finds it hard to win.

Liberty was underlined by natural rights; the rights that everyone can enjoy in nature.[65] Natural rights derive from the divine. The English scholastic philosopher and catholic theologian William of Ockham invoked natural rights to liberty against human laws. Natural rights prevailed over human laws. This was the basis upon which he defended the Franciscan order against interventions by the Pope.[66] Privacy appears at early biblical stories. "Almost the first page of the Bible introduces us to the feeling of shame as a violation of privacy. After Adam and Eve had eaten the fruit of the tree of knowledge, "the eyes of both were opened, and they knew that they were naked; and they sewed fig leaves together and made themselves aprons."' Thus, mythically, we have been taught that our very knowledge of good and evil – our moral

---

[60] William Shakespeare, *Romeo and Juliet,* see https://www.goodreads.com/quotes/272658-what-man-art-thou-that-thus-bescreened-in-night-so.

[61] Eoin O'Dell, *Compensation for Breach of the General Data Protection Regulation* 40(1) Dublin University Law Journal 97 (2017).

[62] B.R. Bale, *Informed Lending Decision v Privacy Interests in Great Britain* 10 Transnational Lawyer 77 (1997).

[63] B.L Cardonsky., *Towards a Meaningful Right to Privacy in the United Kingdom* 20 Boston University International Law Journal 396 (2002).

[64] Beate Roessler, Dorota Mokrosinska, *Social Dimensions of Privacy*, 78 (Cambridge, CUP, 2015).

[65] Richard Tuck, *Natural Rights Theories: Their Origin and Development* (Cambridge CUP, 1979).

[66] Alessandra Facchi, Silvia Falcetta, Nicola Riva, *An Introduction to Fundamental Rights in Europe*, 5 (Cheltenham, Edward Elgar, 2022).

nature, our nature as men-is somehow, by divine ordinance, linked with a sense and a realm of privacy".[67]

Despite the fact that the early teachings of the Christian Church were hostile to individual ownership of property; these teachings against ownership failed to take assume prominence in England where a cultural trend traced back to Aristotle viewed ownership of property as the basis of a durable society.[68] The underlining concept of liberty was the right to personal property. The phrase an Englishman's home is his castle[69] and fortress[70] embodies the profoundness of the right in question. In *Entick*[71] the court clarified that civil liberties entail preventing access to one's property by an agent of the state unless it is expressly provided for by law. Liberty is a sacrosanct right which allows an individual to exercise his activities without any intervention within a space he owns. There is a fundamental)understanding of individual liberty as inextricably linked with ownership of property. That's why George Orwell presented the dystopic reality of modern intensive mass surveillance activities[72] even at one's domicile in vivid terms. "There was of course no way of knowing whether you were being watched at any given moment…all the time…day by day and almost minute by minute the past was brought up to date".[73]

The writings of John Locke encouraged the view that the "purpose of society and government"' was to "further the enjoyment of property, and political power was only legitimate if it served this end".[74] Liberty is based on self-ownership; therefore, on a property right. This is a natural right therefore, it possessed a profound character as it is granted to man by nature; it somehow has a divine character. Human laws just recognised what was already granted to man by nature. Locke argued that "every man has a property in his own person".[75] The limits between what I own and what I am are blurry in the English philosophical tradition if any. That impacts upon both the definition and the concept of privacy as reflected in the English law where there is a link between what can be kept private in a space that we own. Therefore, there was a clear conflict of the essence of property rights between the so-called Anglo-Saxon jurisdictions and the continental European thought on the matter.

---

[67] Milton Konvitz, *Privacy and the Law: A Philosophical Prelude*, 31 Law and Contemporary Problems 1 (1966). See: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3108&context=lcp.

[68] A.G Monks. Robert, Minow Nell, *Corporate Governance*, 96 (Chichester John Wiley and Sons Ltd, , 2010).

[69] *Semayne's* Case (1603) 77 Eng. Rep. 194, 195.

[70] ,R Singh., *Privacy and the Media after the Human Rights Act* 6 European Human Rights Law Review 712 (1998).

[71] *Entick v Carrington* (1765), see: https://www.bailii.org/ew/cases/EWHC/KB/1765/J98.html.

[72] Dorcas Basimanyan, *The Regulatory Dilemma on Mass Communications Surveillance and the Digital Right to Privacy in Africa: The Case of South Africa* 30(3) African Journal of International and Comparative Law 362 2022.

[73] George Orwell, *1984* (1949). Available on line at http://www.online-literature.com/orwell/1984/, accessed on 27 February 2023.

[74] W. Hutton, *The World We're In* (London, Little Brown, 2002).

[75] John Locke, *Two Treatises of Government, Second Treatise*, §§ 25 – 51, 123–26. At: https://press-pubs.uchicago.edu/founders/documents/v1ch16s3.html.

Privacy and Data Protection in the English Law and Case Law

The UK knew no general right of privacy and the Parliament was not willing to introduce one.[76] The right to privacy was adopted in response to "external forces"[77] namely; the European Convention on Human Rights, which was incorporated in the UK law only in 1998 with the Human Rights Act,[78] with which "the right to privacy…acquired binding legal force"[79] requiring "public authorities to respect privacy rights".[80] Thus, before the enaction of the1998 Act it was "well known that in English law there was no right to privacy"[81] as "the right of privacy was first ignored and then expressly disavowed by the judiciary in England and Wales…so long…that it can be recognised now only by the legislature".[82] As Lord Denning had argued "we have as yet no general remedy for infringement of privacy; the reason given being that on the balance it is not in the public interest that there should be one".[83] The Parliament had refused to give the ECHR domestic effect, therefore, British courts "did not vindicate the individual autonomy rights recognised under the ECHR".[84]

Privacy debates involved the actions of the press and media[85] and it was only until the case of *R v Brown*[86] that the spotlight was put on the threats from internet. In *Brown* it was stated that "English common law does not know a general right of privacy".[87] That the individual shall have full protection "in person and in property is a principle as old as the common law".[88] The link between privacy and property was strong. But, "propertising personal information requires the inalienability of

---

[76] Jeremy Morton, *Data Protection and Privacy* 18 (10) European Intellectual Property Review 558-561 (1996).

[77] Francesa Bignami, *Cooperative Legalism and the non-Americanisation of European Regulatory Styles: The Case Of Data Privacy*, 423 (2011). Accessed at the SSRN network: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1813966.

[78] It has to be noted however that the 1998 Human Rights Act refers to the relationship between the individual and the public authorities while the Data Protection Act 1998 covers the relationships between individuals as well.

[79] Emanuel Gross, *The Struggle of a Democracy against Terrorism, Protection of Human Rights: The Right to Privacy versus the National Interest – The Proper Balance* 37 Cornell International Law Journal 82 (2004).

[80] Richard Clayton, Hugh Tomlinson, *Privacy and Freedom of Expression*, 64 (Oxford, Oxford University Press, 2001).

[81] Singh Rabinder, Strachan James, *The Right To Privacy in English Law* 2 European Human Rights Law Review 129 (2002).

[82] Ibid.

[83] *Re X* (1974), [1975] 1 All ER 697 (CA) at 704.

[84] Ronald J. Krotosnynski, *Autonomy, Community and Traditions of Liberty: The Contrast of British and American Privacy Law*, Duke Law Journal 1415 (1990). See it at: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=3136&context=dlj.

[85] Ibid.

[86] *R v Brown* [1996] 1 All ER 545.

[87] *R v Brown* [1996] 1 All ER 545 at 555.

[88] Ida Azmi Madieha*, E-Commerce and Privacy Issues: An analysis of the Personal Data Protection Bill* 8(8) Computer and Telecommunications Law Review 206-212 (2002).

property in a legal system that protects privacy".[89] Based on this premise, the need to introduce a right to privacy was becoming apparent.[90] In 1993 the Calcutt Committee made a link between privacy and the publication of information defining the former as "the right of the individual to be protected against intrusion into his personal life or affairs…by publication of information".[91] In courts the privacy cases were dealt on the basis of the law of confidence whose roots "lie in equity".[92] The law "would protect what might reasonably be called a right of privacy, although the name accorded to it would be breach of confidence".[93] At that point an independent right of privacy from the common law was not likely.[94] The judicial protection granted in cases of privacy was "almost by incident as an incidental effect"[95] of a variety of laws enacted for other purposes. Viewing privacy within the context of a breach of confidence[96] was problematic from many aspects. By using this doctrine to protect privacy, the UK rejected "Warren and Brandeis' view of privacy and chose to protect it from a basis more akin to intellectual property rights".[97] In *Guardian Newspapers*[98] the House of Lords "discarded the requirement of a confidential information. Under the force of Lord Goff of Chieveley's criticism of that requirement as illogical where an obviously confidential document came into the hands of someone with whom the injured party had no confidential relationship"[99] the House of Lords explicitly acknowledged that the concept of confidence had already acquired two forms: The first is related to trade secrets which are accompanied by a duty of confidence flowing from "a transaction or a relationship between parties"[100] and the second one linked

---

[89] Leon Trakman, Robert Walters, Bruno Zeller, *Is Privacy and Personal Data Set to Become the New Intellectual Property?* 50(8) International Review of Intellectual Property and Competition Law 949 (2019).

[90] See also *Kaye v Robertson* [1991] FSR 62, where it was clearly stated that a right of privacy did not exist in the UK legal order. However, an element of a right to privacy was indeed recognised in Morris v Beardmore [1980] 2 All ER 753. Lord Scarman described the right to privacy as fundamental.

[91] Laura Donohue, *Anglo-American Privacy and Surveillance* 96(3) The Journal of Criminal Law and Criminology1154 (2006).

[92] David Bainbridge, *Introduction to Computer Law*, 100 (Fifth Edition, London, Pearson Longman, 2004).

[93] See *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 and R v Department of Health, ex parte Source Informatics Ltd [2001] QB 424.

[94] Loon Wee, *Emergence of a Right to Privacy from within the Law of Confidence?* 18(5) European Intellectual Property Rights Review 312 (1996).

[95] International Commission of Jurists, *The Protection of Privacy* XXIV (3) International Social Science Journal 457 (1972).

[96] See also *Coco v AN Clark*, [1969] RPC 41, where the three requirements for an action of breach of confidence were spelled out. McGarry J stated that the information must have the necessary quality of confidence about it…that information must have been communicated in circumstances importing an obligation of confidence…there must be an unauthorised use of the information to the detriment of the party communicating it.

[97] David Eady, *Injunctions and the Protection of Privacy* 29(4) Civil Justice Quarterly 97 (2020).

[98] *A.G. v Guardian Newspapers Ltd* (No2), [1990] 1 A.C. 109 (H.L.).

[99] Russel Brown, *Privacy Law: Article: Rethinking Privacy: Exclusivity, Private Relation and Tort Law* 43 Alberta Law Review 597 (2006).

[100] *A.G. v Guardian Newspapers Ltd* (No2), [1990] 1 A.C. 109 (H.L.) at 281.

to privacy where a breach of privacy "would be preconditioned upon circumstances where a relationship, whether of confidence or otherwise existed".[101] In landmark *Douglas v Hello* the court stated that "what a concept of privacy does is accord recognition to the fact that the law has to protect not only those people whose trust has been abused, but those who simply find themselves subject to an unwanted intrusion into their personal lives. The law…can recognise privacy itself as a legal principle drawn from the fundamental value of personal autonomy".[102] It was argued that all we need is confidential information and for the "adjective confidential one can substitute the word private".[103] A tort focused more concretely on the misuse of personal information took shape in *Campbell*.[104] Lord Hoffmann in Campbell stated that "what human rights law did was to identify private information as something worth protecting as an aspect of human autonomy and dignity".[105] Thus, the developments mainly at the level of case law "to protect privacy within the existing framework of the common law may well have been in response to government indecision over the recent decades on the issue of privacy".[106] The problem was that "the UK lacked experience in applying fundamental human rights in the constitutional context".[107]

Therefore, there was unease with the passing of the DP Directive. The UK government opposed the directive arguing that it would impose "burdensome obligations on companies",[108] because financial institutions will be heavily affected by such obligations.[109] In order to transpose the directive the UK passed the Data Protection Act 1998.[110] The Data Protection Registrar stated in his 1994 report that "data protection legislation is about the protection of individuals rather than the regulation of industry It is civil rights legislation rather than technical business legislation".[111] It is due to the transposition of the EU directive into the UK legal order that the concept of sensitive data was introduced into English law.[112] Significantly the Registrar has emphasised that the "Directive introduces into English law a right to informational privacy,

---

[101] Russel Brown, *Privacy Law: Article: Rethinking Privacy: Exclusivity, Private Relation and Tort Law* 43 Alberta Law Review 597 (2006).

[102] Sedley LJ, in *Douglas v Hello Ltd*, 2 WLR, 2001, 992 at paragraph 126.

[103] *Douglas*, paragraph 83.

[104] Leon Trakman, Robert Walters, Bruno Zeller, *Tort and Data Protection Law: Are There Any Lessons to Be Learnt?*, 8 (2020). Accessed at the SSRN network at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3630004.

[105] Rebecca Wong, in Mathias Klang and Andrew Murray, *Human Rights in the Digital Age*, 155 (London, Glasshouse Press, 2005).

[106] Mackenzie P. Andrew, *Privacy – A New Right in UK Law* 12 Scots Law Times 98-101 (2002).

[107] John DR Craig, Nolte Nico, *Privacy and Free Speech in Germany and Canada: Lessons for an English Privacy Tort* 2 European Human Rights Law Review 162 (1998).

[108] Fiona M Carlin, *The Data Protection Directive, The Introduction of Common Privacy Standards* 21(1) European Law Review 65 (1996).

[109] Jonathan Moakes, *Data Protection in Europe – Part 1* 1(2) Journal of International Banking Law 77 (1986).

[110] http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

[111] Tenth Annual Report of the Data Protection Registrar, (London, HMSO, 1994).

[112] Ibid.

which is effective since 1998".[113] The rights introduced into English law were entirely new; they did not depend on whether the data subject would have rights under the existing law of confidentiality.[114] As Ian Lloyd puts it, the UK moved from a situation where the data controller can process personal data unless prevented by law, to one where an individual can prevent processing unless the controller can show why this should be permitted.[115]

The DP directive was the first major instrument of EU law that the UK felt unease with as it embodied privacy and data protection principles that the UK legal order did not embrace; however, it was certainly not the last one. A new round of debates came into place with the passing of the ePrivacy Directive[116]with the UK implementing it in a rather minimalist way especially in relation to the controversial in the UK article 5(3) of the directive regarding the "cookie opt-in" obligation. The UK placed its emphasis upon avoiding to add burden to companies in need to get consent for the use of cookies and insisted that prior consent will not be required if the cookie is strictly necessary to deliver a service which has been requested by the user. This was the preferred option on the part of the government which insisted that it allowed the UK to be compliant with the E-Privacy Directive without the permanent disruption caused by an opt-in regime.[117] However, the Commission launched a case against the UK regarding "several problems with the UK's implementation of the ePrivacy directive".[118] The case was suspended as the UK passed subsequent law[119] to remedy the flaws of its implementation but the whole process to get there demonstrates how unease the country felt in implementing the enhanced data protection standards of the EU. If that was the case during its EU membership one can imagine how challenging it will be to maintain adequate levels of data protection post-Brexit.

Brexit and the Way Forward: The UK as a Third Country and the Post-Brexit Legislative Landscape – An Inhospitable Environment for Both Privacy and the Right to Protect Personal Data

Article 45 GDPR (like its predecessor article 25 of the DPD) is the legal basis upon which data can be transferred out of the EU. It is instrumental for trade with the EU

---

[113] IIana Saltzman, Joanna Cassidy, *The Data Protection Directive: How is UK Data Protection Law Affected* 7(3) International Company and Commercial Law Review 110-114 (1996).

[114] Antony White, *Data Protection and the Media*, Special Issue: Privacy 2003, European Human Rights Law Review 25-36 (2003).

[115] Lloyd Ian in White (2003), Ibid.

[116] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[117] BIS Impact Assessment (2010) at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/31568/10-1133-implementing-revised-electronic-communications-framework-impact.pdf.

[118] See the EC's Press Release at: https://ec.europa.eu/commission/presscorner/detail/en/IP_09_570.

[119] See the relevant law at https://www.legislation.gov.uk/uksi/2011/1340/made.

as it requires an adequate level of protection of personal data to allow their transfer to a third country. Therefore, if a third country is deemed as inadequate in its protection of personal data, then trade with the EU becomes a complex matter. This demonstrates the significance of introducing the regulation through the internal market; it rendered an adequate level of data protection a pre-requisite for trade with the EU. The Council of Europe Convention 108 on data protection[120] had previously established a similar mechanism for the flow of personal data with third countries,[121] but due to a lack of enforcement mechanism the latter remained mostly on paper. With the passing of the DPD first and the GDPR now through the internal market aiming at facilitating data flows within it, this mechanism is in force and acts as an international guide for trading with the EU.

The definition of the term "adequacy" of article 25 DPD was provided by the Working Party as "dependent on whether the jurisdiction has a comprehensive data protection law…when private sector data protection laws require the companies to comply with a range of requirements that generally meet the standards set out in the EU Data Protection Directive".[122] The CJEU was instrumental in highlighting the content of the term "adequate" which stands at the core of article 45 GDPR too. The CJEU defined adequate in a strict manner as "essentially equivalent".[123] There needs to be a level of protection "essentially equivalent" to that guaranteed within the European Union now by the GDPR which should be "read in the light of the Charter";[124] this highlights the role of the Charter within the EU legal order but also within the EU's external trade relations. In order for the Commission to adopt an adequacy decision pursuant to Article 45(3) of the GDPR, it must find, duly stating reasons, that the third country ensures, by its domestic law or international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed "in the EU legal order".[125] The *Schrems* ruling clarifies the mechanism behind article 45 which is stricter than the respective of its predecessor article 25 DPD. The court refers to the regulation as read in the light of the Charter; a text which by definition aims at enhanced protection of fundamental rights and freedoms. To place further emphasis upon the fact that the GDPR is only one component of the web of legal texts that need to be examined, the court states that we need evidence of a level of protection of

---

[120] Convention 108 + for the Protection of Individuals with regard to the Processing of Personal Data. See: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[121] Article 14 of the Convention 108 +.

[122] The European Commission, Directorate General Internal Market, A*pplication of a Methodology designed to Access the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer, Final Report*, p165 (Luxembourg September 1998).

[123] *Maximilian Schrems v Data Protection Commissioner and Facebook Ireland*, Case C-311/18 at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=45C7060956BBA7AAA1A949305FD5C275?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1548263.

[124] Paragraph 104.

[125] Paragraph 162.

fundamental rights equivalent not just to the regulation but to the "EU legal order" as a whole. The latter consists of the Treaty which has incorporated the Charter into its body as well as the ECHR through article 6TEU.[126] Therefore, what the court now dictates is essential equivalence to the protection granted by the basic texts of the EU legal order and edifice. The shift from the DPD to the GDPR reflected also the evolution of data protection from a right of data subjects that required legal protection into a fundamental right at the core of the EU legal order upon which any trade relations of the EU with a third country are dependent. Article 16TFEU on the right to data protection embodies the new status of data protection as universal fundamental right within the EU legal order. Hence, we moved from the need to achieve the flexibly drafted "adequate protection" of article 25 DPD into the multi-dimensional and rooted into hard-core EU constitutional texts "essentially equivalent" protection of the GDPR. That serves as a proof of the spectacular rise of data protection from a sparsely discussed concept up to the 1980s, into a regulated right in a few member states in the 1990s, then into a protected right by the DPD and finally into a fundamental right with a constitutional legal basis nowadays.

That has fundamentally changed the landscape within which nations trade with the EU and it has created a huge challenge for the UK especially in the light of the stated intentions of the British government to create its own Bill of Rights and abolish the Human Rights Act which has incorporated most of the ECHR into the British legal order. This will place trade relations between the UK and the EU into serious risks. Right now, there is a very delicate thin line on which the UK may retain the protection of personal data as a fundamental right within its legal order post Brexit. According to article 5(4) of the EUWA,[127] the Charter is not part of the domestic law after exit day. Taking into account that data protection is expressly provided for by the Charter in article 8[128] but it is not explicitly provided for by the ECHR the abolition of the Charter in the UK will likely weaken its status in the British legal order. The abolition of the Charter in the UK has dis-entrenched a strong legal basis for the protection of personal data in the UK. Norms are considered to "be entrenched when they are harder to change than other norms";[129] the EU treaty was an example of that.

In this context it could be argued that according to article 5(5) the removal of the Charter does not affect the retention in domestic law of any fundamental rights or principles which existed in the UK irrespective of the Charter. This would seem to

---

[126] The EU is to respect fundamental rights as guaranteed by the ECHR and Fundamental Freedoms from the constitutional traditions common to the Member States, as general principles of Community law. Those fundamental rights are incorporated in the Charter, with the same legal status as the Treaties. Paragraph 16 of the judgement of *Association Belge des Consommateurs Test-Achats ASBL and Others v Conseil des ministres*.C-236/09, See: https://curia.europa.eu/juris/document/document.jsf?text=&docid=80019&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6199894.

[127] The European Union Withdrawal Act 2018. See https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted.

[128] See the charter at: http://fra.europa.eu/en/eu-charter/title/title-ii-freedoms.

[129] Tobias Lock, *Human Rights Law in the UK after Brexit*, P.L Brexit Special Issue, 119 (Nov 2017).

be the legal basis upon which the protection of personal data may operate in the UK. However, as explained in detail in the previous part of the article defining even the umbrella right of privacy as a "fundamental right" was quite challenging in the UK before 1998. Since, the charter is no longer enforceable in the UK, then the British legislator may indeed interpret article 5(5) of EUWA as not relevant to privacy at all as it did not exist as a fundamental right in the English legal culture. The CJEU may continue to protect privacy and personal data as fundamental rights[130] and third countries need to adhere to those standards but the post-Brexit UK will not have to follow any of the decisions of the CJEU[131] and more importantly there is no right of action in domestic law after exit day based on a failure to comply with any of the general principles of EU law such as privacy and data protection.[132]

The Fragile "Adequacy Decision" and the Bumpy Road Ahead

Post-Brexit the UK enjoyed a rather unique status as the only former member of the EU with 40 years of experience of implementing EU law with full compliance with EU law and standards due its previous membership. Therefore, it was thought that attaining the status of "essentially equivalent" legal standards would be easy. That was wrong. In June 2021 the EU adopted two adequacy decisions on the UK; one under the GDPR[133] and one under the Law Enforcement Directive.[134] The decision found that the UK GDPR[135] and the DPA 2018[136] ensure a level of protection for personal data that is essentially equivalent to the one guaranteed by Regulation (EU) 2016/679.[137] The adequacy decision is based on both the relevant UK domestic regime and its adherence to the ECHR and submission to the jurisdiction of the European Court of Human Rights. Continued adherence to such international obligations is

---

[130] Diana Sancho, *The Concept of Establishment and Data Protection Law: Rethinking Establishment* 42(4) European Law Review 491 (2017).

[131] Article 6(1)(a) of the EUWA 2018.

[132] Schedule 1, paragraph 3(1) of the EUWA 2018.

[133] See https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[134] See https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_law_enforcement_directive_en.pdf.

[135] The UK GDPR, as incorporated into the law of the United Kingdom under the European Union Withdrawal Act 2018 and amended by the Data Protection Privacy Electronic Communications Regulations 2019. See: https://www.legislation.gov.uk/ukdsi/2019/9780111177594/contents Per recital 16 of the "Adequacy Decision" as the UK GDPR is based on EU legislation, the data protection rules in the United Kingdom in many aspects closely mirror the corresponding rules applicable within the European Union.

[136] This is the UK legislation implementing the GDPR: See https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted It was amended by section 4 and schedule 2 of the Data Protection Privacy Electronic Communications Regulations 2019 to ensure GDPR compliant flow of data within the UK. See: https://www.legislation.gov.uk/ukdsi/2019/9780111177594/schedule/2.

[137] Recital 273 of the adequacy decision. Supra note 127.

therefore a particularly important element of this decision.[138] The commission noted[139] that the UK has committed to remain party to the ECHR[140] and to Convention 108 of the Council of Europe,[141] the only binding multilateral instrument on data protection. This means that, while it has left the EU, the UK remains a member of the European "privacy family".[142] The commission notes that this is of particular importance for the stability and durability of the adequacy findings. Recital 281 of the decision provides us with two grounds on which the decision may be suspended or repealed. This will happen firstly if the UK legal framework on data protection is reformed in divergence with the respective EU law and secondly and quite importantly if the UK enters into agreements with third countries over the use of personal data that may undermine the protection of EU data subjects.

Despite those clear grounds for the suspension of the decision, the British government did not hide its intentions to withdraw from the ECHR and to amend the current data protection framework. Since 2014 there have been a few calls on the part of the ruling Conservative Party to abolish the HRA 1998 and introduce a new "bill of rights". In the relevant proposals it is clearly stated that the HRA "undermines the sovereignty of the parliament".[143] The proposals which have been discussed up until now aim at "breaking the link between the British courts and the EcHR" and end the "ability of the EcHR to force the UK to change its law".[144] The government aims at passing a British Bill of Rights and in case of no agreement with the Council of Europe that the latter is in implementation of the ECHR in the UK, then it will withdraw from the ECHR.[145] The exact content of such a bill is not yet known and therefore, it is not clear as to whether it will reflect the content of the ECHR; one can assume that this will not be the case as otherwise the UK would simply not consider its departure from the convention. In a purely British bill of rights, one may again assume that rights which were not traditionally viewed as "fundamental rights" in the UK such as the right to privacy or to data protection may not be granted a status equivalent to that within the EU legal order. The UK placed more emphasis on freedom of expression and "less on the balancing right to privacy than continental jurisdictions".[146] In three

---

[138] Recital 277 of the adequacy decision. Supra note 127.

[139] Press Release of 19/2/2021 on the Draft Adequacy Decision. See: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

[140] See the convention at: https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=.

[141] See the convention at: https://www.coe.int/en/web/data-protection/convention108-and-protocol.

[142] Press Release of 19/2/2021 on the Draft Adequacy Decision. See: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_661.

[143] Protecting human rights in the UK. *The Conservatives' Proposals for Changing Britain's Human Rights Laws* at 4 (October 2014). See: https://www.theguardian.com/politics/interactive/2014/oct/03/conservatives-human-rights-act-full-document.

[144] Ibid at 6.

[145] Ibid at 8.

[146] Rupert Earle, Ross Allan, Andrew Wheelhouse, *Brexit – The Impact on Media Law* 27(7) Entertainment Law Review 230 (2016).

cases *Kennedy*,[147] *Osborn*[148] and *Moohan*,[149] the English courts "have asserted the precedence of the application of existing common law rights rather than having recourse to the HRA. They have criticised counsel for paying little attention to domestic administrative law and have effectively invited advocates…to rely on domestic common law instead of norms stemming from an international source".[150] It was emphasised that "common law "did not come to an end on the passing of the Human Rights Act 1998"[151]

That will impact upon the status of adequacy as the adequacy decision made a clear link between the HRA of 1998 and the protection of both privacy and data protection in the UK. In recital 10 it was explicitly noted that the HRA of 1998 incorporates the rights of the ECHR into the law of the UK. This includes the "right of respect to for private and family life[152] and the right to data protection as part of that right".[153] Should the new bill of rights do not reflect that, then the decision may be repealed with considerable impact on trade.[154]

The retention of personal data for "national security" in the UK post-Brexit. Could it make the trade between the EU and the UK more insecure?

A field of possible post-Brexit divergence in legal standards may rest in the field of retention of data by national security authorities. The English courts were traditionally hesitant to find police actions of collecting and retaining private data as "prima facie breach of privacy rights".[155] In *MM V UK*,[156] the EcHR described this judicial approach as "generous". Nowadays, the use of personal data in the context of national security falls out of the GDPR, but the Commission noted a blanket exception will still be closely examined.[157] In *Digital Rights Ireland*,[158] the Court of Justice invalidated

---

[147] *Kennedy v Charity Commission* [2014] UKSC20.

[148] *Osborn v Parole Board*, [2013] UKSC 61.

[149] *Moohan v Lord Advocate* [2014] UKSC 67.

[150] Veronika Fikfak, *English Courts and the "Internalisation" of the ECHR? Between Theory and Practise* (2015). See https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2616394.

[151] *R (Guardian News and Media Ltd) v City of Westminster Magistrates' Court* [2012] EWCA Civ 420, [88] (Toulson LJ).

[152] Article 8 of the ECHR.

[153] Recital 10 of the adequacy decision. See: https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[154] An indication of the future direction of the British legislature is the proposed "Illegal Immigration Bill". In section 1(5) it states that "section 3 of the HRA 1998 does not apply in relation to the provisions of the Bill". This may indicate that future bills will undermine the application of the HRA and consequently of the ECHR even if the latter is not fully repealed. See: https://publications.parliament.uk/pa/bills/cbill/58-03/0262/220262.pdf.

[155] Lilian Edwards, *Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence?* 24(3) International Journal of Law and IT 304 (2016).

[156] *M.M. v. the United Kingdom* – 24029/07 Judgment 13.11.2012 [Section IV].

[157] Lorna Woods, *Data Protection, the UK and the EU: The Draft Adequacy Decisions* (24 February 2021). See: http://eulawanalysis.blogspot.com/2021/02/data-protection-uk-and-eu-draft.html.

[158] *Digital Rights Ireland Ltd* (C293/12), see: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0293.

the 2006 Data Retention Directive,[159] which required the retaining of electronic metadata for law enforcement purposes for a considerable period of time.[160] The decision imposed restrictions on the national data retention schemes. The UK had previously put in place the Data Retention Regulations 2009[161] which implemented the now defunct directive. To adapt to the new landscape post – *Digital Rights Ireland*, the UK adopted the DRIPA 2014[162] which provided for data retention in the UK for law enforcement aims. Since, this was emergency legislation it expired in 2016 only to be replaced by IPA 2016.[163] But, the CJEU in the *Tele2 Sverige* and *Watson*[164] found that the EU Charter[165] precludes national legislation which allows general and indiscriminate retention of all traffic and location data of all users for fighting crime purposes. The charter has emerged as a solid legal basis for the protection of personal data; this is linked with the previous analysis on the impact of its abolishment in the post-Brexit UK legal order. Therefore, the court found that the indiscriminate data retention regime created by the DRIPA 2014 was in breach of EU law, thus "de facto making the provisions of the IPA 2016 void too".[166] The adequacy decision somehow did not consider this as grounds on which equivalence would not be granted, but the CJEU may indeed adjudicate to demolish part of the decision if its rulings are not complied with. The *Schrems II* case serves as a clear reminder of that. In addition to that, the European Parliament criticised the broad immigration exception within the UK law. The parliament argued that the UK Data Protection Act 2018[167] provides for a general exemption for the processing of personal data for immigration purposes; when non-UK citizens' data "(including EU citizens) are processed then, they are not protected in the same manner as UK citizens.[168] The EP notes that this does not amount to adequate protection of personal data and it reiterates its position that this should be remedied before an adequacy decision is reached.[169]

---

[159] Directive 2006/24 on the retention of data generated [2006] OJ L105/54. See: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[160] See Marie-Pierre Granger and Kristina Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection* 39 European Law.Review 834 (2014).

[161] See https://www.legislation.gov.uk/ukdsi/2009/9780111473894/contents.

[162] The Data Retention and Investigatory Powers Act 2014, see: https://www.legislation.gov.uk/ukpga/2014/27/contents/enacted.

[163] Investigatory Powers Act 2016, see: https://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

[164] Joined Cases *Tele2 Sverige AB v Post- och telestyrelsen* (C203/15) and *Secretary of State for the Home Department v. Watson* (C698/15), See: https://privacyinternational.org/sites/default/files/2019-08/CELEX_62015CJ0203_EN_TXT.pdf.

[165] Articles 7, 8 and 11 and Article 52(1).

[166] Edoardo Celeste Data Protection in Federico Fabbrini (ED), *The Law & Politics of Brexit: Volume III: The Framework of New EU-UK Relations*, 203 (Oxford, OUP, 2021).

[167] Sch 2, 1 (4).

[168] EP Resolution of 12/2/2020, paragraph 32. See: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0033_EN.html.

[169] European Parliament resolution of 21 May 2021 on the adequate protection of personal data by the United Kingdom (2021/2594(RSP)), See: https://eur-lex.europa.eu/legal-content/EN/TXT/

In *Open Rights Group*[170] the court of appeal held that the immigration exception was incompatible with the UK GDPR. This case revealed the very complex legal environment post-Brexit. According to section 5(2) of the EU Withdrawal Act 2018,[171] the principle of the supremacy of EU law in the UK seizes to exist except on EU-derived law still in the British statute books; such piece of legislation that still benefits from the principle of supremacy is the therefore the UK GDPR. Article 5 of the UK GDPR[172] is reflective of the respective EU GDPR provision regarding the principles related to the processing of personal data that include a transparent and fair processing of the data in question and its collection for specified, explicit and legitimate purposes compatible with those purposes. However, article 23 of the UK GDPR opens a window of exception to that by "means of legislative measure".[173] That means that the text of the regulation putting in place strict conditions upon which personal data can be processed can be altered through domestic law aiming at satisfying a widely defined end of "national security". This amounts to a potential radical watering down of the legal standards introduced by the regulation. The latter is a rather rigid legal tool applying in its entirety across member states. However, post-Brexit the UK, has already opened the window for its gradual reform towards relaxing its standards. A further legal basis to relax those standards can be found in article 8 of the EU Withdrawal Act 2018[174] which allows to mitigate "deficiencies in retained EU law (such as the UK GDPR) by regulation". In this context the UK passed the Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations of 2022.[175] Per the 2022 regulations, the immigration exemption applies to rights in the UK GDPR which can be restricted to the extent that giving effect to those rights would be likely to prejudice the maintenance of effective immigration control or to the investigation of activities that would undermine the maintenance of effective immigration control. The rights that can be restricted are those of article 5 of the UK GDPR.[176] Therefore, the core of the data protection legislation has now a basis of derogation; immigration control in the context of national security. As a gesture of not breaking the links with the EU, the immigration exemption can be applied only by the Secretary of State and not by other data controllers. This demonstrates political

---

PDF/?uri=CELEX:52021IP0262.

[170] *The Open Rights Group & Anor, R (On the Application Of) v The Secretary of State for the Home Department & Anor (Rev2)* [2021] EWCA Civ 800 (26 May 2021), http://www.bailii.org/ew/cases/EWCA/Civ/2021/800.html.

[171] See: https://www.legislation.gov.uk/ukpga/2018/16/section/5#:~:text=(2)Accordingly%2C%20the%20principle,%5BF1IP%20completion%20day%5D.

[172] See https://gdpr-info.eu/art-5-gdpr/.

[173] See https://gdpr-info.eu/art-23-gdpr/.

[174] See https://www.legislation.gov.uk/ukpga/2018/16/section/8/enacted#:~:text=8Dealing%20with%20deficiencies%20arising%20from%20withdrawal&text=arising%20from%20the%20withdrawal%20of%20the%20United%20Kingdom%20from%20the%20EU.&text=(g)contains%20EU%20references%20which%20are%20no%20longer%20appropriate.&text=(b)a%20deficiency%20in%20retained,a%20Minister%20of%20the%20Crown.

[175] See https://www.legislation.gov.uk/uksi/2022/76/contents/made.

[176] See https://gdpr-info.eu/art-5-gdpr/.

motivation on the UK part to keep some balance with its EU law-flowing obligations in the field.

In this context and despite the aforementioned developments, the Commission proceeded with the adequacy decision in any case, while excluding personal data to which the immigration exemption applied from the scope of the decision.[177] This shows that the commission also demonstrated strong political will to grant the equivalence status to the UK even if that meant that it would overlook the serious concerns regarding the retention of data, mass surveillance[178] and immigration. This is despite the fact that UK authorities appear to be "considerably less constrained with regard to introduce surveillance and investigatory tools".[179] The adequacy decision may walk on thin ice as two of the union's main institutions seem to be discontent with it which can be translated into lack of tolerance about any future divergence from the current status quo on the part of the UK.[180]

Can the USA Come in between the EU and the UK?

Regarding the second basis for repealing the adequacy decision, there is a need to examine the "data adequacy partnerships"[181] between the UK and third non-EU countries. This may emerge as the indirect avenue through which the personal data of EU citizens may pass to countries with no equivalence status; the most notable example of them being the USA which the UK names as "priority partner".[182] The *Shrems*[183] decision invalidated the Privacy Shield agreement between the EU and the USA on the basis of the Charter. Should a potential agreement between the UK and the US fall below the EU legislative standards, which appears to be likely, then the impact of that agreement on the adequacy decision of the commission on the UK will be grave. This creates a paradox; while the UK attained an opt-out from the Charter

---

[177] Recital 6 of the decision. See https://commission.europa.eu/system/files/2021-06/decision_on_the_adequate_protection_of_personal_data_by_the_united_kingdom_-_general_data_protection_regulation_en.pdf.

[178] The respective EU-USA agreement was structed down by the CJEU in *Schrems II* on similar basis of the potential misuse of EU citizens personal data by the US national intelligence authorities.

[179] David Cole, Federico Fabbrini, *Bridging the Transatlantic Divide? The United States, the European Union and the Protection of Privacy Across Borders* 14(1) International Journal of Constitutional Law 226 (2016).

[180] The proposed Data Protection and Digital Information Bill which is currently still debated will be scrutinised in its final form for its conformity with the decision. See: https://bills.parliament.uk/bills/3322.

[181] See https://www.gov.uk/government/news/uk-unveils-post-brexit-global-data-plans-to-boost-growth-increase-trade-and-improve-healthcare.

[182] See Peter Swire, *UK's Post-Brexit Strategy on Cross-Border Data Flows* at: https://www.lawfareblog.com/uks-post-brexit-strategy-cross-border-data-flows.

[183] *Maximilian Schrems v Data Protection Commissioner and Facebook Ireland*, Case C-311/18 at: https://curia.europa.eu/juris/document/document.jsf;jsessionid=45C7060956BBA7AAA1A949305FD5C275?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1548263.

during its membership in the EU, it will find it very difficult to escape the extra-territorial application of the Charter on the international flows of personal data in its post-Brexit relationship with the EU.

Up to now the UK had upheld the EU stance against data flows to the USA despite the rhetoric. In September 2023 the UK-US Data Bridge[184] was finally agreed.[185] This was a positive step towards remaining within the widely defined European privacy family. This is because these Regulations specify the United States of America as a country which provides an adequate level of protection of personal data for certain transfers according to the UK law.[186] The UK basically extended the respective EU-US agreement on the matter thereby converging with the EU stance on this very crucial matter. This means that personal data which will be in the scope of the EU-US Data Privacy Framework Principles[187] which was agreed in July 2023; data can be transferred to persons in the United States of America who participate in the UK Extension to the EU-US Data Privacy Framework without the need for any specific authorisation. The Framework is not without challenges and looking at the recent past when similar agreements have been plunged to oblivion by the CJEU it remains to be seen what the UK stance may be in case the EU policy is subject to a radical shift.

All this clearly demonstrates that the UK has to operate in an international environment greatly shaped by the EU data protection standards. By placing data protection at the core of its internal market policy and subsequently at the heart of its external trade relations, the EU emerged as the defining jurisdiction in the global data protection landscape; by 2017 over 100 jurisdictions had adopted such a law mostly influenced by the EU blueprint.[188] This has created a status of supremacy by default[189] for the EU data protection model. The threat of "complete or partial market closure"[190] suffices for a state with significant market power to impose its "regulatory preferences"[191] on other states. In fact, "normative convergence has by and large emerged in the field of data protection around the world"[192] as a by-product of the EU data protection model. The EU law emerged as the "gold standard" of data protection regimes as the EU has "essentially influenced how the world thinks about data protection" and

---

[184] See https://assets.publishing.service.gov.uk/media/650801f6fc63f60014957399/analysis_of_the_uk_extension_to_the_eu-us_data_privacy_framework.pdf.

[185] See https://www.legislation.gov.uk/uksi/2023/1028/made.

[186] For the purposes of Part 2 of the Data Protection Act 2018 ("the 2018 Act") and the UK GDPR (defined in section 3 of the 2018 Act).

[187] See https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en.

[188] David Erdos, *European Data Protection Regulation, Journalism and Traditional Publishers*, 44 (Oxford, OUP, 2019).

[189] Olga Lynskey, *The Foundations of EU Data Protection Law*, 43 (Oxford, OUP, 2015).

[190] Daniel Drezner, *All Politics is Global: Explaining International Regulatory Regime* 32 (Princeton, Princeton University Press, 2007).

[191] Yuko Suda, *The Politics of Data Transfer*, 23 (New York, Routledge, 2018).

[192] Yilma Kinfe, *Privacy and the Role of International Law in the Digital Age*, 101 (Oxford, OUP, 2023).

became the "effective sovereign of global privacy law".[193] We are now at a stage where data protection laws will be "ubiquitous in that they will be found in almost all economically more significant countries".[194] By 2020 there were 130 countries with data protection laws with a large majority of the laws by then coming from outside Europe.[195] In this context any country with no "adequate" or "equivalent" regime of data protection to that of the EU will gradually evolve into the pariah of the global trade system. Countries like the USA can survive through maintaining their individual arrangements due to their immense size (although EU-like laws are passed at State level even in the USA), but the UK will find it hard to prosper outside this framework.

The UK has "significantly less leverage over the EU than the US with disrupted data flows impacting citizens in the UK significantly more than those in the EU".[196] The EU is the main trade partner of the UK. The EU represents more than 50% of the UK's trades in goods and services.[197] In addition to that, the UK technology and digital sector is now worth more than $1 trillion and it is the third internationally only after the USA and China.[198] In this very context three-quarters of the UK's cross border data flows are with the EU[199] and services account for 44% of the UK's total global exports.[200] 49% of the UK's exports are to the EU.[201] Among G-20 countries, the UK's digital economy is now the largest at 10% of its GDP; it is now the UK's second-biggest economic contributor behind the property sector, having overtaken manufacturing and retail.[202] Taking into account these figures, it is of vital importance for the UK to conform with the data protection legal standards of the EU despite Brexit.

---

[193] Leonie Wittershagen, *The Transfer of Personal Data from the European Union to the United Kingdom Post-Brexit*, 299 (Berlin, De Gruyter, 2023).

[194] Graham Greenleaf, *Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories*, accessed at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280877.

[195] Ibid.

[196] Clowance Wheeler Ozanne, *Dear or No Deal: Does It Matter? Data Protection Predictions for Post-Brexit Britain* 24(2) Edinburgh Law Review 279 (2020).

[197] Issam Hallak, *Future EU-UK Trade Relationship, European Parliament*, 6 (February 2020), See: https://www.europarl.europa.eu/cmsdata/210518/EPRS_BRI(2020)646185_EN.pdf.

[198] Press release, *UK Tech Sector Retains #1 Spot in Europe and #3 in World as Sector Resilience Brings Continued Growth* (Department for Digital, Culture, Media and Sport, 21 December 2022). See: https://www.gov.uk/government/news/uk-tech-sector-retains-1-spot-in-europe-and-3-in-world-as-sector-resilience-brings-continued-growth.

[199] The House of Lords, European Union Committee. *Brexit: The EU Data Protection Package,* 3rd Report of Session 2017-19, published 18 July 2017 (HL Paper 7). See: https://publications.parliament.uk/pa/ld201719/ldselect/ldeucom/7/702.htm.

[200] Ibid.

[201] Issam Hallak, *Future EU-UK Trade Relationship, European Parliament*, 6 (February 2020). See: https://www.europarl.europa.eu/cmsdata/210518/EPRS_BRI(2020)646185_EN.pdf.

[202] Report of the Boston Consulting Group, *The Internet Contributes 10% of GDP to UK Economy* (RNS Number : 9487L, May 2015). See: https://www.investegate.co.uk/the-boston-consult/rns/the-internet-contributes-10 – of-gdp-to-uk-economy/201505010700289487L/.

Will the New "Data Protection and Digital Information Bill" of 2024 Jeopardise the Adequacy Decision?

After multiple years of debates and extensive negotiations the DPDI Bill[203] has passed its second reading before the House of Lords and in January 2024[204] it approached the stage of its final reading. Despite the rhetoric preceding the Bill, it was encouraging to read the explanatory note at the very beginning of the Bill where Viscount Camrose made the statement that per the undersection 19(1)(a) of the Human Rights Act 1998 in his view the provisions of the Data Protection and Digital Information Bill are compatible with the ECHR rights. Despite the fact that the ECHR rights are explicitly inclusive only of the right to privacy but not of the right to data protection, the reference to the ECHR can only be viewed as positive. Firstly, because it negates any intention to withdraw from the Convention and secondly because it guarantees the application of the umbrella right to privacy. The Bill is to amend parts of the Data Protection Act 2018 and the UK GDPR. There are two issues to consider here. Firstly, the Bill may still be subject to amendments which can further delay its introduction in its final form therefore rendering any analysis of its provisions a risky project. Hence, the bibliography on this matter is up to now scarce if any. Secondly, it can be said that the initial declarations on the part of members of the government that the Bill will amount to a radical re-shape of the current data protection regime do not appear to reflect the reality. Having said that, this does not mean that the Bill does not appear to introduce a watering-down of some standards of the two aforementioned laws. Whether the changes which are presented and explained here will be viewed by the EU as grounds to revoke the adequacy decision remains to be seen.

The most notable change is the re-definition of "personal data" into "information related to an identifiable living individual"[205] by Clause 1 of the Bill. The same provision makes a distinction between direct or indirect identification of the data subject. An individual is identifiable from information "directly" if the individual can be identified without the use of additional information. In the case of direct identification, the living individual is identifiable by the controller or processor by reasonable means at the time of the processing. On the other hand, an individual is identifiable from information "indirectly" if the individual can be identified only with the use of additional information".[206]

This provision can lead to a potentially significant lowering of legislative standards as it adds a "test of reasonableness" to the identification of the data subject. The basic question here is: why do we need this test if the data subject can be identified anyway? This defies the whole purpose of protecting personal data in the sense of not having the capacity to link them to an individual in the first place. This stands at the core of both the GDPR and of the Convention 108+ as well as at the core of the Data

---

[203] See https://bills.parliament.uk/publications/53287/documents/4126.
[204] See https://bills.parliament.uk/bills/3430.
[205] See https://bills.parliament.uk/publications/53287/documents/4126.
[206] Article 1(1)(b) of the Bill.

Protection Act 1998 and the UK GDPR. The Bill as a whole does not seem to diverge from the current data protection standards to a preoccupying degree but it can be argued that divergence at the very definition of what personal data is may undermine the whole data protection edifice as it alters the very subject matter of the relevant protection. Paragraph 106 of the explanatory notes raises more issues regarding the definition of personal data and the test of reasonableness. It states that the term "by reasonable means" includes any means that the controller is likely to use, taking account of, amongst other things, the time, effort and cost to identify an individual from the information. The technology that is available to the person or organisation that is processing the information is also likely to be a relevant factor. Other factors, such as whether steps taken to identify or re-identify data subjects would be lawful and or proportionate in a particular situation may be relevant to the overall assessment of reasonableness. Therefore, one can deduce that if the data controller amounts to a small entity which does not possess these means, then this may entail the ability of the controller in question to process the data as if it does not amount to personal data. That will deprive the data subject from the protections of article 5 of the UK GDPR.[207] In contrast to that, if the controller amounts to a large entity in possession of the appropriate resources and technology then, the same data may be deemed to be personal and subject to such protections. This would create uncertainty in relation to which data is to be protected, inequality in the applicable standards and dependence on the individual capacities of the controller in question. This brings the UK in conflict not only with the EU law but also with its international commitments as it is in breach of article 2 of the Convention 108 which defines personal data as "any information relating to an identified or identifiable individual".[208]

In the case of indirect identification where the controller or processor knows, or ought reasonably to know, that another person will, or is likely to, obtain the information as a result of the processing, and the living individual will be, or is likely to be, identifiable by that person by reasonable means at the time of the processing. In this case the Bill implies that additional information will be needed for the data subject to be indirectly identified. The pseudonymisation of data may fall within the scope of indirect identification. Paragraph 101 of the explanatory notes[209] states that the legislation does not apply to non-personal or anonymous data, so the purpose of this clause is to provide greater clarity about which type of data is in scope of the legislation.

In addition to that clause 2 of the bill on research and statistical purposes[210] amends article 4 of the UK GDPR to include "any research that can reasonably be described as scientific". The term "reasonably" will need to be further highlighted by practise and future case law. However, it can be assumed at this point that the wording is

---

[207] See https://gdpr-info.eu/art-5-gdpr/.

[208] See https://rm.coe.int/1680078b37.

[209] See https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265en.pdf.

[210] See https://bills.parliament.uk/publications/53287/documents/4126.

inclusive of a greater range of commercial and non-commercial activities that could be identified as research.

More importantly the Bill amends article 6(1)(f) of the UK GDPR on the lawfulness of processing. Clause 5 of the Bill introduces the notion of "recognised legitimate interests" of the controller as defined by Annex 1 to include matters of national security, defence and the fight against crime. Quite importantly, the Secretary of State may add or omit the conditions of the Annex without the need of primary legislation, therefore enlarging the capacity of the controller to process data either based on the set of grounds set by the Bill or on the basis of the future grounds that may be introduced by the Secretary of State. That entails an expansion of the legal ability of the controller to process personal data even in the case of children. The balancing test of the article 6(1)(f) of the UK GDPR has been effectively weakened to a great extent.

Clause 17 amends Article 35 of the UK GDPR and section 64 of the DPA 2018 from "Data Protection Impact Assessments" to 'Assessments of high-risk processing'. The Data Protection Impact Assessments of the UK GDRP will no longer be mandatory; only high-risk processing would require an assessment. In conjunction with that Clause 17 (2) amends the heading of Article 35 of the UK GDPR and section 64 of the DPA 2018 from "Data Protection Impact Assessments" to 'Assessments of high-risk processing'. The Bill now apparently states that the DPIA will no longer be mandatory but instead only high-risk processing would require an assessment.

Clause 7 amends Article 12 of the UK GDPR. Clause 7 (3) inserts into the UK GDPR a new Article 12A. Article 12A permits a controller to charge a reasonable fee for or refuse to act on a request which is 'vexatious or excessive'. This replaces the previous provision in Article 12 to refuse or charge a reasonable fee for 'manifestly unfounded or excessive' requests. Therefore, article 12(5) of the UK GDPR which allowed the subjects' requests to access their personal data to be rejected if found to be "manifestly unfounded or excessive" has been relaxed significantly. The identification of the request as "vexatious" will suffice as grounds to reject the request. The new article 12A (5) of the UK GDPR as amended by Clause 9 of the Bill introduces the quite wide, fluid and flexible notion of "bad faith" too. If the request is not found to be in good faith, then, it can be rejected. Therefore, the test relies on criteria which become more challenging in their exact definition therefore, enlarging the scope of the controller to reject the request.

Clause 14 replaces the requirements on Data Protection Officers in Articles 37 to 39 of the UK GDPR and sections 69 to 71 of the DPA 2018. Clause 14 (2) adds a new Article 27A to the UK GDPR. New Article 27A (1) sets out the criteria for when a senior responsible individual needs to be appointed, namely where the controller or processor is a public body or where they are carrying out processing that is likely to result in a high risk to individuals. Organisations would therefore no longer need to appoint a senior responsible individual if their processing activities were defined as "low risk"; this yet another change from the UK GDPR regime. These changes appear to move the UK away from the strict provisions of the GDPR as implemented by the UK GDPR. However, it has to be noted that the legislative text as it stands now does not seem to amount to the radical break away from the EU law standards as previously

feared. Whether the EU will come up to the same conclusion when revisiting the Adequacy decision remains to be seen.

Conclusion

The article looked at privacy and data protection in the UK post-Brexit. In order to understand the complex relationship between the English and the EU notions of privacy and then of data protection the article examined in detail the historical, cultural and legal background of the doctrines in question. The English legal order perceived privacy in very different ways than the European one and that created unease even during membership. Brexit gives the opportunity of breaking with the EU legal norms in the field. The article argued that this will be wrong. The nature and structure of the British economy is heavily based on the free flow of data between the UK and the EU. Data flows are the lifeline of both the digital economy as well as the trade in services where the UK excels. It is imperative that the UK continues to embrace the principles that it gradually forged in its legal culture since 1998. This is instrumental for its economic well-being. Any radical departure from the data protection standards of the EU in a "lighter-touch"[211] direction will be translated into severe trade turbulence and consequently into an economic crisis. The UK already paid a price in giving up the free movement of goods and services within the world's biggest single market. If the loss of the free movement of data – the lifeblood of the UK's economy and trade relations – is added to that -intentionally or by accident – then, the impact upon its economy will be severe. Opting for conformity with the EU standards does not only amount to a sensible choice from an economic point of view, but it also perhaps equally significantly maintains the level of protection of human rights and fundamental freedoms of the British citizens too. The application of the ECHR in the UK guarantees to a degree an enhanced level of protection not just of the rights in question but of the whole bundle of rights consolidated by the convention. Forging economic prosperity and uninterrupted trade flows while maintaining a high level of protection of human rights is by far the most sensible choice.

[211] James Clark and Alexandra Greaves, *Brexit: Key Impacts on Data Protection* 19(1) Privacy & Data Protection 7 (2018).