Rights of Data Subjects in the United Kingdom and the European Union

Meyirbek Abdikadirov*, Amirkhon Rakhmatkariev, Sarvarbek Olimjonov, Dilshodbek Orifjonov
Westminster International University, Tashkent, Uzbekistan.

* Corresponding author. Email: abdikadirovmeyirbek@gmail.com (M.A.)

Manuscript received April 19, 2023; accepted July 6, 2023; published August 9, 2023.
DOI: 10.18178/IJBTA.2023.1.1.15-22

Abstract: In the digital age, the collection and processing of vast amounts of personal data have made it necessary to establish legal frameworks that protect the rights of individuals. This legal essay provides an overview of the existing data subject rights in the UK and EU, with a focus on the right to erasure on blockchain and the right not to be subject to automated decision-making in respect of artificial intelligence. The paper examines the legal framework surrounding these rights as well as any potential challenges or limitations they may face in practice. The right to erasure on the blockchain is explained, including its benefits and drawbacks, and its interaction with data protection laws in the UK and EU. The right not to be subject to automated decision-making is also discussed, including the legal framework surrounding this right, as well as its relationship with artificial intelligence and data protection laws. The implementation of these rights is essential in safeguarding individuals' privacy and promoting trust in the use of technology. Although there may be barriers preventing individuals from fully exercising these rights, legal remedies such as increased awareness and transparency, as well as changes to the law and harsher consequences for noncompliance, can help to mitigate these obstacles.

Keywords: Data subject rights in the UK and EU, right to erasure on blockchain, right not to be subject to automated decision-making, artificial intelligence, blockchain

1. Introduction

In the digital era with the proliferation of new technologies and the vast amounts of personal data they generate, it has become imperative to establish clear legal frameworks to protect the rights of individuals whose data is being collected and processed.

This legal essay aims to provide an understanding of all the existing data subject rights in the UK and EU with a particular emphasis on the right to erasure on blockchain and the right not to be subject to automated decision-making in respect of artificial intelligence. We will explore the legal framework surrounding these rights, as well as any potential challenges or limitations they may face in practice.

2. Date Protection across Borders: Rights of Data Subjects in the EU and UK

2.1 An Insight into the Regulatory Landscapes of the EU and UK

The EU and UK legal regimes of data subjects are closely related although have forged different paths since Brexit. The UK has deviated from the EU regime in several respects, including the UK's permissive approach to data transfers [1], the introduction of a new supervisory authority – ICO [2], and modification in standards for national security and law enforcement [3].

Nevertheless, the key regulatory tools, namely the EU GDPR [4] and the UK's GDPR [5] along with the Data Protection Act 2018, are essentially the same. Considering extensive data flows between the EU and the UK, such analogous data protection laws are of high relevance [6].

2.2 The Right to Be Informed

The right to be informed obligates data controllers to provide individuals with detailed information (privacy notices) about how their personal data is being collected, processed, and shared [7]. Failure to comply with imposed obligations leads to monetary [8] and reputational repercussions [9].

The right to be informed is a critical feature of data protection, ensuring that individuals have the knowledge required to make informed decisions about their personal data. However, the majority is yet unaware of their right to be informed [10]. Ensuring that organizations provide transparent and accessible privacy notices, coupled with educating the public on data protection, is vital to foster informed decision-making and safeguarding individual privacy.

2.3 The Right to Access

Individuals have the right to request access to their personal data held by data controllers. This right is designed to empower individuals to have greater control over their personal information and to ensure that data controllers are held accountable for the use of personal data [11].

To exercise this right, individuals must submit a request to the data controller, who must provide a copy of the requested data free of charge and without delay [12]. However, certain exemptions and restrictions apply concerning data affecting other individuals or national security [13].

Failure to comply with a valid access request enables the requestor to complain to the data protection authority [14] and seek redress through the courts.

Despite the importance of the right to access for ensuring transparency and accountability in data processing, practical and legal challenges frequently arise. Organizations must be aware of the hazards associated with disclosing personal data, including unauthorized access or personal information misuse [15]. These risks emphasize the necessity of vigilance in monitoring and enforcing the right to access to guarantee its effective implementation.

2.4 The Right of Rectification

The right of rectification is a right of an individual to have incomplete or erroneous personal data altered upon their request [16]. This right is closely related to the controller's duty to guarantee that personal data is correct, up-to-date and dealt with in a timely manner if it is inaccurate [16]. 'Inaccurate' [17] personal data means any data which is misleading as to matters of fact [18]. Such an ambiguous definition can provoke a number of troublesome situations, where there is confusion regarding what falls under 'inaccurate' personal data [19].

2.5 The Right to Restrict Processing

Data subjects have the right to limit the way their personal data is utilized [20]. This right is not absolute and can only be requested in a handful of instances [20]. These instances encompass situations when personal data is inaccurate [21], the processing of personal data is unlawful [22] or when an individual requires personal data for managing a legal claim. If processing restrictions have been requested, controllers may store the individual's personal data, but not process or use it [22].

Although the list of circumstances when this right can be invoked is exhaustible, problems can still arise if it is unclear that this personal data falls under the definition of 'inaccurate'. One of the potential solutions for this dilemma is making data controllers rather than individuals responsible for proving whether personal data is accurate [23].

2.6 The Right to Data Portability

An ability to receive and reuse personal data across various services is granted by the right to data portability [24]. The essence of this right is that it allows data subjects to move, copy and transmit their personal data from one controller to another in a simple, safe and efficient manner [24]. The right to data portability has one of the most substantial implications, as online data providers envisage that it can help considerably decrease the operational costs for consumers who are willing to switch from one digital service market to another [25]. Nonetheless, as the research reveals, the implementation of this right is in need of urgent attention since currently this innovation is only known to a small percentage of individuals [25].

2.7 The Right to Object

Ultimately, a data subject may invoke the right to object to prevent an organisation from processing or utilising its personal data [26]. However, it might be challenging to object since an organisation might have legitimate grounds to use an individual's personal data. Thus, this right is only applicable in specific instances [26]. For example, an individual may object to the processing of their personal data when an organisation exploits this data in the public interest, in the exercise of public authority or for historical, statistical, or marketing purposes [26].

3. Right to Erasure and Challenges on Blockchain

3.1 Understanding Blockchain: The Basics and Beyond

A blockchain is a decentralized, synchronized database that is shared by many nodes and upheld by a consensus process.

As blockchains are intended to accomplish durability through replication, a large number of people are frequently involved in keeping these databases up to date. Each node has the ability to independently maintain the database and keeps an integral replica of it [27]. These systems use a **decentralized** data collection [28], storage and processing approach [29]. Blockchains are also append-only ledgers [30], meaning that data may only be added to them and erasure or alteration is almost impossible [31].

3.2 The Right to Erasure in the Age of Blockchain

The right to erasure [32], also known as the 'right to be forgotten' is an essential right of individuals that provides them with the control to exercise over their personal data [33]. Considering the immutable nature of blockchain technology, implementation of this right on a blockchain poses several challenges, including:

1) Governance challenges [34] that are considered as the most complex issues to achieve the privacy objective. Even if there are multiple technical solutions to implement the right to erasure on blockchain technology, it seems impossible to comply with data subject rights because of the communication and coordination mechanisms between the actors involved in processing the data [35].
2) Blockchain technology is well-known for its **immutability** which means that once data is stored on the blockchain, it cannot be erased or altered. Hence, this system makes it difficult to exercise the right to erasure within the technology since the data stored is decentralized and several copies exist [36].
3) There are **limitations on the territorial scope** [37] of the right to erasure under GDPR, which also can be defined as a jurisdictional legal and regulatory challenge. All jurisdictions have (or do not have at all) their own legislation and legal framework for such technologies [38]. There is no uniform and universal legal framework that can be applicable to all states. The importance of this challenge is that blockchain technology has a cross-jurisdictional character. Since GDPR applies only within the territory of the European Union, outside the territorial jurisdiction, it would be hard to implement such a right [39].

3.3 The Right to Erasure and Blockchain: Navigating the Challenges and Opportunities

The following legal solutions should be implemented to address the aforementioned issues relating to the Right to Erasure and the challenges that arise concerning blockchain technology:

There should be an adoption of a new law which prohibits storing data on blockchain: The issues with the right to erasure on blockchain may be solved by enacting new legislation that restricts the addition of personal data to the blockchain network. The storing of private data shall be prohibited on the blockchain so that the right to erasure can be enforced. While enacting new legislation that bans the addition of personal data to the blockchain may be a solution, it should be carefully considered in light of the potential advantages and obstacles of the technology and balanced with other legal and technical solutions to address the issues with the right to erasure on the blockchain.

1) Universal jurisdiction [40]. As it is stipulated that there are certain limitations on territorial jurisdiction and all states have conflicting legislation on blockchain technology, it would be a good solution if there is a universal legislation that can be applied to all states' territories so that blockchains can be designed to comply with data protection laws.

2) Legal responsibilities and liabilities [41]. Rules or laws might be implemented to specify the responsibilities and liabilities of organizations that keep individuals' data on blockchains. This might involve implementing the proper organizational and technical safeguards to secure personal information and guarantee compliance with data protection laws.
3) Consent of the individuals [42]. Getting individuals' explicit consent before storing their personal information on the blockchain can help in upholding the right to erasure. Individuals must be informed about the risks associated with storing private data on the blockchain as well as how their data will be utilized. If there is a law on obtaining consent from an individual whose data is being stored, this law will help to ensure the right of the people under GDPR.
4) Transparency [43]. Consequently, organizations may make their usage of personal data on the blockchain more transparent to enable users to decide whether to contribute their data. This may entail giving brief and explicit explanations of the blockchain's scope and goals as well as the procedures for gathering, storing, and using personal data.

3.4 Conclusions on the Right to Erasure on Blockchain

After careful examination of the difficulties and restrictions of various approaches, it is evident that the right to erasure cannot be fully realized in the context of blockchain technology. Rather, promoting transparency and educating the public about how their data is used on the blockchain network is the most viable solution. In conclusion, even though the right to erasure might not be possible on the blockchain, increased transparency and understanding can guarantee better data protection for people.

4. Right not to Be Subject to Automated Decision-Making in Respect of Artificial Intelligence

4.1. The Rise of Automated Decision-Making: Opportunities and Challenges

Automated decision-making (ADM) about artificial intelligence (AI) is a concept that involves the utilization of algorithms and machine learning technologies to automate decision-making processes without the intervention of humans. ADM is defined as "any decision which is taken solely by automated means without any human involvement, including profiling" [44].

While the usage of such technology attracts more and more companies due to its potential efficiency and cost savings benefits [45], resulting the lack of human involvement in these decision-making processes can raise concerns about transparency, accountability, and fairness [46].

This chapter will explore the importance of the right not to be subject to AMD, including its exceptions, as well as relevant cases and potential risks. It will also analyze regulatory measures to exercise this right and provide recommendations for addressing system flaws.

4.2. The Right Not to Be Subject to Automated Decision-Making: A Human Rights Perspective

The use of ADM in certain contexts can lead to flawed decision-making processes, causing frustration and confusion for individuals. For example, rejection emails for job applications or loan applications generated by an algorithmic process can leave individuals feeling powerless and helpless [47].

It's essential to note that the right not to be subject to ADM becomes critical in such cases [48]. To illustrate the perils associated with ADMs, two examples shall be viewed: facial recognition technologies [49] which are used for collecting personal data without the consent of subjects, and tools such as the COMPAS algorithm, which has been used to predict reoffending [50]. However, Article 22(2) of the GDPR describes a few exceptions [51] to the right not to be subject to ADM that have a legal or similarly significant effect [52]:

1) Where the decision is necessary for entering into or performing a contract between the data subject and the controller (i.e., the entity responsible for processing personal data).
2) Where the decision is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
3) Where the decision is based on the data subject's explicit consent.

These exceptions must be clearly defined and limited in scope to ensure that they do not undermine the

right not to be subject to ADM [53].

4.3. Empowering Individuals: How to Exercise the Right Not to Be Subject to ADM?

The effective exercise of the right not to be subject to ADM entails following specific steps that enable individuals to safeguard their privacy and prevent unfair or biased decision-making processes [54]. The primary step involves submitting a request to the controller, the data processing entity, or the data protection officer [55]. The request must not only state the individual's objection to ADM in line with the provision [56], but it should also explicate the grounds for the objection and preference for human intervention in the decision-making process [57]. ICO and EDPB [58] are the UK and EU Supervisory Authorities respectively that enforce data protection rules. Notably, there is lot of criticism towards these authorities [59] for lacking resources [60] and enforcement powers to hold companies accountable for ADM violations [61].

4.4. Rethinking ADM Regulations: Addressing Emerging Challenges and Opportunities

To deal with all abovelisted uncertainties, it is suggested to establish a new legal framework that is tailored to address the unique challenges concerning ADM.

Firstly, legal frameworks could be created that mandate organizations to obtain explicit consent [62] from individuals before deploying ADM to make important decisions, or that provide individuals with a right to challenge automated decisions before a human decision-maker.

Secondly, there shall be mandatory transparency [63] requirements included in GDPR, so companies could be required to disclose information to the ICO or EDPB, as well as to data subjects.

Moreover, by increasing the fines [64] for non-compliance companies may be more motivated to invest in measures to ensure compliance rather than risk facing hefty penalties.

4.5. Reflections on the Right Not to Be Subject to ADM and AI

The right not to be subjected to ADM is paramount in preventing biased and unjust AI decision-making procedures.

To this end, GDPR allows for exceptions to this right, but these exceptions must be limited in scope. Any such exceptions must be balanced against the need to protect individual rights and freedoms.

To address concerns about ADM regulations, legislative changes such as new frameworks, transparency standards, and increased penalties for noncompliance are necessary. It will all certainly play a role in mitigating the risks associated with ADM.

It is significant to strike a balance between the advantages and hazards of ADM, while also upholding individual rights. As we continue to develop and implement ADM technologies, it is crucial that we remain vigilant in protecting individual rights. Only then we could be certain that ADM is utilized for the greater good, rather than as a tool for discrimination or oppression.

5. Conclusion

In conclusion, data protection regimes in the UK and EU seek to ensure that individuals have control over their personal data and that organizations use it in a responsible and transparent manner. The implementation of these rights, including the right to erasure on blockchain and the right not to be subject to automated decision-making, is essential in protecting individuals' privacy and promoting trust in the use of technology.

While there may be barriers preventing individuals from fully exercising their rights, these barriers can be lessened via the use of legal remedies like increased awareness and transparency as well as changes to the law and harsher consequences for noncompliance.

A balance between the advantages and disadvantages of technology must be struck while upholding individual rights in our increasingly data-driven society. Data protection rights are fundamental human rights, and their protection must be a top priority in our digital age.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Meyirbek Abdikadirov: Edited and combined all parts, structured the content, organized the process, designated responsibilities among the authors, and collected necessary sources. Amirkhon Rakhmatkariev: Assisted with editing, focused on general data subjects' rights, and actively participated in the process. Sarvarbek Olimjonov: Conducted research and provided insights on the topic of "The Rise of Automated Decision-Making: Opportunities and Challenges." Dilshodbek Orifjonov: Conducted research and wrote about the challenges and opportunities related to the right to erasure in the context of blockchain technology in the section titled "The Right to Erasure and Blockchain: Navigating the Challenges and Opportunities." All authors approved the final version of the paper.

References

[1] C. Kuner and L. A Bygrave, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2016. Andrew D Murray, 'Data Protection Law, Proportionality and the Public Interest' (2014) 4(1) International Data Privacy Law 2.

[2] Information Commissioner's (2021). Office. *Data Protection and Brexit.* [Online]. Available: https://ico.org.uk/for-organisations/data-protection-and-brexit/

[3] Joseph Cannataci and Emma Llansó, 'Reconciling Data Protection and National Security: Finding the Right Balance' (2016) 2(1) European Data Protection Law Review 7; Gloria González Fuster, 'The EU General Data Protection Regulation: Toward a Property Regime for Protecting Personal Data?' (2015) 22(1) Columbia Journal of European Law 29.

[4] European Union General Data Protection Regulation 2016/679 (EU GDPR).

[5] United Kingdom General Data Protection Regulation, Retained Regulation (EU) 2016/679 (UK GDPR).

[6] Paul De Hert, Vagelis Papakonstantinou and Yves Poullet, 'The EU General Data Protection Regulation: Toward a More Coherent Data Protection Framework in Europe' (2013) 29(2) Computer Law & Security Review 130.

[7] GDPR (both regimes), arts 13 and 14; DPA 2018, s 7.

[8] EU GDPR, art 83; DPA 2018, s 115.

[9] Information Commissioner's Office, 'Right to be informed' (*ICO*, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/> accessed 23 February 2023.

[10] Fabiana Di Porto and Daniele Catteddu, 'Privacy and Personal Data Protection in the Digital Era: An Overview of the EU General Data Protection Regulation' (2018) 26(1) International Journal of Law and Information Technology 1.

[11] Sonam Mittra, 'The Right to Access Personal Data: A Comparative Study of the GDPR and the Data Protection Act 2018' (2019) 4(1) Journal of Intellectual Property Rights and Allied Sciences 56.

[12] GDPR (both regimes), art 15; DPA 2018, s 7.

[13] Giuseppe Mazziotti, 'The Right of Access under the GDPR: A Critical Analysis of the Limitations and Exceptions' (2021) 12(2) European Journal of Law and Technology 10; Information Commissioner's Office, 'Right of access' (*ICO*, 2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/> accessed 3 March 2023.

[14] In the UK, the relevant authority is the ICO, whereas in the EU, it varies by member state.

[15] Laura Drechsler, 'The Right of Access under the GDPR: An Appraisal of the Notion of Disproportionate Effort' (2021) 7(1) European Data Protection Law Review 38.

[16] Thomson Reuters, 'Right to rectification of personal data' (Practical Law, 2023) <https://uk.practicallaw.thomsonreuters.com/w-014-8203?transitionType=Default&contextData=(sc.Default)&firstPage=true> accessed 8 March 2023.

[17] DPA 2018, s 2.

[18] Information Commissioner's Office, 'Right to rectification' (*ICO*, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/> accessed 8 March 2023.

[19] Paulan Korenhof, 'The Right to Rectification under the GDPR and the Directive on Data Protection: One Step Forward, Two Steps Back?' (2017) 3(4) European Data Protection Law Review 446.

[20] Information Commissioner's Office, 'Right to restrict processing' (*ICO*, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-

regulation-gdpr/individual-rights/right-to-restrict-processing/> accessed 8 March 2023.
[21] Gianclaudio Malgieri, 'The Right to Restrict Processing under the GDPR: A Fundamental Right in Search of Protection' (2019) 5(1) European Data Protection Law Review 24.
[22] Nikos K Michalopoulos, 'Restrictions on Processing Personal Data under the GDPR: An Overview of the Regulatory Landscape' (2018) 2(2) Journal of Data Protection & Privacy 123.
[23] Orla Lynskey, 'Restricting the Processing of Personal Data: Balancing Data Subjects' Rights and Controllers' Interests under the GDPR' (2018) 43(2) European Law Review 234.
[24] Janis Wong and Tristan Henderson, 'The right to data portability in practice: exploring the implications of the technologically neutral GDPR' (2019) 9(3) International Data Privacy Law 173 <https://doi.org/10.1093/idpl/ipz008> accessed 8 March 2023.
[25] Sophie Kuebler-Wachendorff *et al.*, 'The Right to Data Portability: conception, status quo, and future directions' (2021) 44(1) Informatik Spektrum 264 <https://link.springer.com/article/10.1007/s00287-021-01372-w> accessed 8 March 2023.
[26] Information Commissioner's Office, 'The right to object to the use of your data' (*ICO*, 2023) <https://ico.org.uk/for-the-public/the-right-to-object-to-the-use-of-your-data/> accessed 8 March 2023.
[27] Thomas Buocz *et al.*, 'Bitcoin and the GDPR: Allocating Responsibility in Distributed Networks' (2019) 35(2) Computer Law & Security Review 182 <https://doi.org/10.3389/fbloc.2020.00026> accessed 4 March 2023.
[28] Emma McClarkin, 'Report on Blockchain: a forward-looking trade policy' (*European Parliament*, 2018) <https://www.europarl.europa.eu/doceo/document/A-8-2018-0407_EN.html> accessed 4 March 2023.
[29] Nabeel Khan *et al.*, 'Proposed Model for Secured Data Storage in Decentralized Cloud by Blockchain Ethereum' (2022) 11(1) Electronics 3686 <https://doi.org/10.3390/electronics11223686> accessed 4 March 2023.
[30] History saved on their own database.
[31] Matthias Berberich and Malgorzata Steiner, 'Blockchain technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers?' (2016) 2(1) European Data Protection Law Review 422 <https://doi.org/10.21552/EDPL/2016/3/21> accessed 4 March 2023.
[32] GDPR 1996, art 17.
[33] Gloria González Fuster, 'The Right to Be Forgotten and the Right to Erasure under EU Data Protection Law: Different Logics and Different Concepts' (2015) 1(2) European Data Protection Law 227.
[34] Michele Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2019).
[35] Lokke Moerel, 'Blockchain & Data Protection and Why They are not on a Collision Course' (2018) 26(6) European Review of Private Law 825 <https://doi.org/10.54648/erpl2018057> accessed 4 March 2023.
[36] Nadezhda Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law' (2018) 10(1) Law, Innovation and Technology 40 <https://doi.org/10.1080/17579961.2018.1452176> accessed 4 March 2023.
[37] Michele Finck, 'Blockchain and the General Protection Regulation: Can distributed ledgers be squared with European data protection law?' (European Parliamentary Research Service 2019) <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> accessed 4 March 2023.
[38] Luis-Daniel Ibáñez *et al.*, 'On Blockchains and the General Data Protection Regulation' (University of Southampton 2018) <https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf> accessed 4 March 2023.
[39] Martin Florian *et al.*, 'Erasing Data from Blockchain Nodes' (Humboldt University of Berlin 2019) <https://www.researchgate.net/publication/332522148> accessed 4 March 2023.
[40] Luiza Dinu and Michalis Vasilomanolakis, 'Towards a universal data protection law for blockchain' (2019) 36(3) Computer Law & Security Review 100367.
[41] Andreas Dorfleitner and Rainer Hornuf, 'Data Protection Compliance in Decentralized Systems: The Example of Blockchain' (2018) 20(3) International Data Privacy Law 211.
[42] Hui Zhong *et al.*, 'Privacy by Consent: Integrating GDPR with Blockchain' (2019) 8(2) IEEE Access 26486.
[43] Dimitra D Dikaiou and Pavlos F Georgiadis, 'Transparency in blockchain-based data processing: can the GDPR be satisfied?' (2019) 35(4) Computer Law & Security Review 465.

[44] GDPR, art 22.
[45] Ajay Agrawal *et al.*, 'Artificial Intelligence: The Ambiguous Labor Market Impact of Automating Prediction' (2019) 33(2) The Journal of Economic Perspectives 31 <https://www.jstor.org/stable/26621238> accessed 23 February 2023.
[46] Bruno Lepri *et al.*, 'Fair, Transparent, and Accountable Algorithmic Decision-making Processes' (2018) 31(4) Philosophy & Technology 611 <http://dx.doi.org/10.1007/s13347-017-0279-x> accessed 23 February 2023.
[47] Swati Sachan *et al.*, 'An explainable AI decision-support-system to automate loan underwriting' (2019) 144(1) Expert Systems with Applications 113 <https://doi.org/10.1016/j.eswa.2019.113100> accessed 23 February 2023.
[48] Aziz Z Huq, 'A Right to a Human Decision' (2020) 105(1) Virginia Law Review 611 <https://chicagounbound.uchicago.edu/journal_articles?utm_source=chicagounbound.uchicago.edu%2Fjournal_articles%2F10159&utm_medium=PDF&utm_campaign=PDFCoverPages> accessed 23 February 2023.
[49] Bridges v South Wales Police [2020] EWCA Civ 1058.
[50] Loomis v Wisconsin [2016] Wis 881 NW2d 749.
[51] EU GDPR, art 22.
[52] European Commission, 'Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679' (*European Commissio*n, 22 August 2018) <https://ec.europa.eu/newsroom/article29/items/612053> accessed 19 February 2023.
[53] Stephan Dreyer and Wolfgang Schulz, 'The General Data Protection Regulation and Automated Decision-making: Will it deliver?' (Bertelsmann Stiftung 2019) <https://www.reframetech.de/en/wp-content/uploads/sites/23/2019/01/GDPR_withoutCover-1.pdf> accessed 19 February 2023.
[54] Rania El-Gazzar and Karen Stendal, 'Examining How GDPR Challenges Emerging Technologies' (2020) 10(1) Journal of Information Policy 237 <https://www.jstor.org/stable/10.5325/jinfopoli.10.2020.0237> accessed 10 February 2023.
[55] Information Commissioner's Office, 'Right to object' (*ICO*, 2023) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/> accessed 19 February 2023.
[56] GDPR, art 22(1).
[57] General Data Protection Regulation, art 22(1).
[58] European Data Protection Board.
[59] The New York Times, 'Europe's Privacy Law Hasn't Aged Well' (*The New York Times*, 27 April 2020) <https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html> accessed 21 February 2023.
[60] European Data Protection Board, 'Lack of resources puts enforcement of individuals' data protection rights at risk' (*EDPB*, 13 January 2022) <https://edpb.europa.eu/news/news/2022/lack-resources-puts-enforcement-individuals-data-protection-rights-risk_en> accessed 23 February 2023.
[61] Michael Veale *et al.*, 'When Data Protection by Design and Data Subject Rights Clash' (2018) 8(2) International Data Privacy Law 105 <https://dx.doi.org/10.2139/ssrn.3081069> accessed 23 February 2023.
[62] Bryce Goodman and Seth Flaxman, 'Regulating Automated Decision-Making: Towards a Right to Explanation' in S G Finlay and K E Whittaker (eds), Proceedings of the 2016 Conference on Fairness, Accountability, and Transparency (New York, ACM 2016).
[63] Lokke Moerel and Titus Corlateanu, 'Transparency Requirements for Artificial Intelligence under the General Data Protection Regulation' (2019) 5(1) European Data Protection Law Review 87.
[64] Maja Brkan, 'Artificial Intelligence and European Data Protection Law: Compliance Challenges and Solutions' (2019) 3(1) Journal of Data Protection and Privacy 76.