УДК 341.645.5

YURIY LI
Master of Commercial and Corporate Law,
Adviser of
the Rector of the Academy of Law Enforcement
Agencies under the
General Prosecutor's Office of the Republic of
Kazakhstan

EUROPEAN UNION LEGISLATION ON THE PROTECTION OF PERSONAL DATA (ЗАКОНОДАТЕЛЬСТВО ЕВРОПЕЙСКОГО СОЮЗА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ)

Түйін. Деректерді қорғау туралы заңнаманы реформалау бойынша жүргізіліп жатқан таластар ұзақ уақытқа созылды. Қазіргі уақытта жеке деректерді қорғау Еуропалық Деректерді қорғау директивасымен (95/46/ЕС) кепілдік берілмейді, себебі оның принциптері ескірген. Жаңа заң осы директиваның кемшіліктерін жеңуге және онлайн шынайылыққа қатысты мәселелерге жауап беруге тиіс. Бұл мақалада жеке деректердің Еуропалық Одақ заңнамасына сәйкес қалай қорғалатыны туралы мәселе қаралады және талданады. Сондай-ақ, Деректерді қорғау туралы директиваға сәйкес жеке деректердің қорғалуын қамтамасыз етуге, сондай-ақ заманауи онлайн әлеміне сәйкес жаңа құқықтық базаның қажеттілігіне назар аударылатын болады.

Түйінді сөздер: Деректерді қорғау туралы Еуропалық Одақтың Директивасы 95/46/ЕС, жеке деректерді қорғауға арналған адам құқығы, Интернет пайдаланушылары, дербес деректерді өңдеу, жаңа технологиялар, Еуропалық Одақтың азаматтары, Еуропалық Одақтың электронды коммерция бойынша 2000/31ЕС55 директивасы.

Аннотация. Непрекращающаяся дискуссия вокруг реформирования законодательства о защите данных затянулась слишком надолго. Защита персональных данных сегодня не гарантирована Директивой Европейского Союза о Защите Данных (95/46/ЕС), поскольку ее принципы устарели. Настала пора реформировать действующее законодательство в этой области. Новый закон должен преодолеть пробелы названной Директивы и ответить на вызовы онлайн - действительности. В этой статье будет рассмотрен и проанализирован вопрос о том, как персональные данные могут быть защищены в соответствии с законодательством Европейского союза. Также будет уделено внимание гарантированию защиты персональных данных согласно Директиве о Защите Данных, а также аргументирована необходимость новой правовой базы в соответствии с современным онлайн - миром.

Ключевые слова: Директива Европейского Союза о Защите Данных 95/46/ЕС, права человека на защиту персональных данных, пользователи Интернета, добыча персональных данных, новые технологии, граждане Европейского Сою-

за, Директива Европейского Союза об Электронной Коммерции 2000/31/EC55.

Annotation. The ongoing discussions about reforming data protection laws across the European Union took far too long. The protection of personal data is no longer adequately guaranteed by the Data Protection Directive (Directive 95/46/EC) as the principles in the Directive are outdated. It is now high time that the laws are reformed. The new legislative regime will overcome the weaknesses of the Directive and meet the challenges posed by new online developments. This article will consider and analyze the issue of how personal data can be protected in accordance with the legislation of the European Union. Also, attention will be paid to guaranteeing the protection of personal data in accordance with the Data Protection Directive, as well as the need for a new legal framework in accordance with the modern online world.

Keywords: European Union Data Protection Directive 95/46 / EC, human rights for the protection of personal data, Internet users, personal data mining, new technologies, citizens of the European Union, European Union directive on e-commerce 2000/31 / EC55.

Introduction

It widely agreed that much debate has been generated around the issue of the Data Protection Directive, as it is said to offer inadequate guarantees on the protection of personal data [5]. The original idea of the Data Protection Directive (DPD) was to facilitate regulation of the progression of personal data across EU member states. The DPD is a European Union Directive, officially known as Directive 95/46/EC. It was devised to augment EU human rights and privacy laws, EU legislation regarding data protection having first been written in 1995; its enactment was intended to guarantee data protection rights, which are regarded as fundamental within the EU. Despite this basic commonality, each member state has implemented their national laws relating to data protection differently, and the complex interpretations have created legal uncertainty and led to increased costs in the administration of this legal principle. Such inconsistency has inevitably resulted in reduced trust and confidence, and thereby impaired the economic effectiveness of the EU. Part of the problem is that the laws were drafted when the online world was starting to get going and the various contentious issues such as data protection did not yet exist. There were no smart cards, smart phones, social media or cloud computing, but the creation of these entities has resulted in a massive increase in the processing of personal data, so new rules are needed in the digital age to ensure people's individual data protection.[5] Such rules could benefit the growing digital economy rather than restrict it. This paper will therefore look at this question, analysing how these concepts can be protected under European Union law. The paper will also investigate how the Data Protection Directive might guarantee personal data protection, and argue the case for a new legal framework being needed to bypass the Directive's outdated law and create new legislation to match the modern online world.

1. The importance of data protection

It seems that there is a common misconception amongst Internet users is that their searches and actions are known only to them. However, there are enormous amounts of information collected on each and every user. Each website visit leaves a trace of where the visitor is from in terms of what sort of computer they have, and who their Internet provider (IP) is, as sites keep visitor logs [6]. This factor shows the size of the overriding issue that the rapid growth of the Internet has created, the prevailing factor being that the worldwide web is a transport network for digital information. Developing technology has massively affected data collection concerning the speed with which

data can be accessed, distributed and analysed. The burgeoning area of e-commerce has been founded on the rapid collection of data, which has been described as: «Data mining – gathering, collating and organising information concerning one's customers and trading partners – is of fundamental importance to all forms of e-commerce.» [6] Each consumer has their own profile, created through the collection of data linked to their searches and purchases. This then results in a marketing strategy being devised to suit the apparent needs of the consumer. Inevitably, much of the information collected is private, so this mining of data constitutes an invasion of cyberspace privacy. The speed of operation of search engines means that they yield mountains of data on any consumer, which businesses can analyse and cross-reference data that might at first appear to be unrelated. [6] This illustrates how important data mining is becoming, with its ability to: «transform... large volumes of random data into meaningful interpretable information, which enables the amelioration of customer service and satisfaction». [6] Identifying a consumer's individual preferences results in a bespoke sales policy design. For example, instead of investing in a blanket marketing strategy for potential gardening enthusiasts – where some Internet users will be keen gardeners but many won't – a company can access a database of consumers who have accessed gardening websites or subscribe to gardening publications. This allows the precise focus by the marketing department or company on consumers who they know are interested in a particular product or area of activity. However, this mass storing of personal information has resulted in the danger of data being misused or falling into the hands of unscrupulous operators.

2. The purpose of the Data Protection Directive

It is commonly known that in 1995, the European Union created a directive called The Data Protection Directive, or DPD. This Directive enables the regulation of personal data processing across the EU, and forms a valuable plank of EU human rights law. The Directive defines personal data as:

«any information relating to an identified or identifiable natural person («data subject»); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity».[1]

"Personal data", under the broad definition, encompasses whatever information is linked to a particular person, such as banking details, bank and credit card numbers, address details, any criminal records data. Some of this data may not even be accessible to the person to whom it relates. Processing in this context means:

«any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction». [2]

The data "controller", i.e., the person, agency, or authority that decides how and why this personal data is to be processed, has responsibility for complying with the appropriate legislation. [5] The rules relating to data protection apply not only to data processing by a controller within the EU, but also to any data processing activity that is undertaken on equipment situated within the EU. [5] Any controllers who are outside the EU must comply with EU regulations in processing information relating to data within the EU. The essence of the original legislation was that online trading involving EU residents would necessarily process data via equipment housed within the EU – through a customer's personal computer, in other words. The website operator would therefore have to follow European data protection legislation. However, the Directive

was devised before the huge expansion of the Internet, so the relevant jurisprudence is so far fairly limited.

3. Application of the Directive

It is argued that this Directive was one of the first EU laws to try and establish a consensus of practice regarding data protection laws, although it was years before individual member states actually implemented it. [5] There are still areas of contention around whether individual countries' courts and data protection authorities have introduced the tenets of the Directive. [5] Originally, the DPD was intended to address the way in which large computer databases processed personal information, and in doing so, it created the legal concepts of "data processor" and "data controller". [4] The Directive brought in further rules concerning how sensitive data, which needed specific consent under Art. 8 of the DPD, was to be processed, and it also dealt with rules relating to the movement of personal data to countries outside the EU. [4] The implementation of the DPD in individual member states has mostly happened through countries amending their existing data protection laws or passing new laws, but national courts have still been charged with confronting this issue. The Swedish courts famously brought the case of Lindqvist [3] before the European Courts of Justice (ECJ), in a test case that sought to probe the extent to which the DPD had jurisdiction over online matters. Although this case clarified the DPD's scope, the outcome was not particularly welcomed. Sweden subsequently altered its extant data protection laws by making use of the exceptions that were written into its Swedish Personal Data Act, thereby adopting the misuse-orientated approach. [13] The law in this area is still subject to challenge, but the ECJ has helped to steer the path of implementation of the DPD as concerns online activity. The big issue is the actual interpretation of the idea of 'personal data', and the question of how the issues around personal data are put into practice remains a subject of great controversy. Regardless of whether a country's law meets the DPD, there are all manner of administrative issues to address when users seek to enforce their rights. For example, if a data controller from within the EU but outside the UK compromises a data subject's security, however unwittingly, and the data subject cannot effectively enforce their rights without recourse to the UK Supervisory Authority, the data protection law itself may be undermined. The issue is not whether data controllers can deal properly with complaints about data protection, through effective mechanisms; the problem is the amount of barriers that an online user may have to surmount in order to access their rights under the Data Protection Directive. One solution to this might be to allow adversely affected online users to follow the Product Liability model, whereby the relevant law would be that law that is in force in the country where the damage has happened. This scenario would better allow data subjects to have recourse to their rights. [8] A prominent example of personal information misuse is the issue of Facebook's operation in Ireland. The Irish Privacy Commissioner audited Facebook to try and determine how well they adhered to data protection and online privacy rules. Although Facebook came out of the audit fairly well, broad changes were recommended to improve users' privacy on the social media giant. [1] The recommendations included involving users more in choices over how their details and information are used on the site, allowing users to see how their data are used by advertisers to target them, and enabling users to have more control over how data relating to them is used on an everyday basis. [9] Although the audit ruled that Facebook should be able to use customer data in advertising, it recommended that the customers should have some power of veto on whether links should be allowed to connect with their profile. [9]

4. The existing weaknesses of the Directive

It is found that safeguarding the data protection rights of all EU nationals while upholding Art. 9 of the DPD is a balancing act.[5] Member states' national legislation allows each country some freedom of interpretation, as countries' own national courts and laws decide how the DPD may be applied. The 'right to be forgotten' is an important right for some people, and the practical application of the DPD is likely to be tested if more people seek to exercise this right. Although the principle of 'the right to be forgotten' is a good one, data protection authorities should have clear guidelines about how this could be implemented to block any misuse of the right, as well as contingency plans to deal with a potential flood of claims about deleting personal data. The question of consent is widely debated currently: some member states require written consent, while others accept the idea of 'explicit' consent. The European Commission needs to clarify the question, especially as regards behavioural advertising, in which Internet browser settings determine the consent of the user. How much users understand various Internet settings is also a matter of consideration: Internet users are very familiar with big companies such as Google and Amazon, but how much detail they know about internet security is unknown. For example, many sites install a pop-up dialogue box that invites the user to acknowledge that they approve of 'cookies', but how many users know what cookies are? The dialogue box will then state that continued use of the site indicates a user's consent; this may be regarded as explicit consent. 'Sensitive data' is another area that needs to be looked at in view of modern developments, including whether genetic data should be thus included. A case could be made for including genetic data under the heading of 'health data' under Art. 8, so the need to make specific reference to this is unclear, while there are perhaps more grounds to include financial data or clickstream data in the review.[7] The revision of the Data protection Directive 95/46/EC has included much debate about the "cloud", and how to bring it under the scope of the European data protection framework. This question illustrates the difficulty of writing legislation to cope with rapidly changing areas of technology, of which data protection is just one area. Hon et al. contend that applying existing data protection laws to cloud computing is not practical, and that when defining 'personal data' the DPD must consider a realistic identification risk in devising data protection rules, which should be based on the actual danger of harm and the degree of severity of harm. [10] Another argument is that the providers of cloud computing should be regarded as neutral; their potential immunity from data protection rules should be addressed by the Electronic Commerce Directive 2000/31/EC55. This directive exempts Internet service providers (ISPs) from specific liabilities through the establishment of particular defences. It is important to note that recently Europe has made a major stride towards more grounded, pan-European data protection laws with the content of new changes. The new data protection rules include the General Data Protection Regulation, which represents the utilization and security of EU citizens' information, and the Data Protection Directive, which represents the utilization of EU residents' information by law implementation. [11] The new rules also mean to make solid data protection regulations for Europe's 500 million residents, streamline enactment between the 28 part states pushing an advanced market and help police and security participation.[11] It is set to supplant the obsolete national regulations that have taken into consideration insignificant fines in cases of infringement. In such a case it seems that reforming data protection laws across the European Union is approaching to the final steps on its way to the new legislative regime that aims to overcome the current weaknesses of the Data Protection Directive.

Conclusion

Thus, in the near future the Directive is likely to be revised, but it must be remembered that on the Data Protection Directive's introduction in 1995, there were difficulties in applying and understanding the Directive through the existing data protection laws of individual countries. The present framework of data protection has been much clarified and strengthened since then. However, current hot topics such as cloud computing and behavioural advertising will lead to grey areas in how to apply the forthcoming Directive, and the limits of the application. Realism is the key to applying the Directive cohesively: if data protection authorities use discretion and considered judgement to weigh individuals' personal information against organisations' legitimate commercial strategies, a balance can be achieved. Despite the Data Protection Directive being long overdue for an overhaul, the new legislation should be fluid in nature, so that data controllers do not have to deal with restrictive and stifling definitions. However, data controllers need to be very aware of the need to protect users' data in this era of widespread social media, cloud computing and behavioural, highly targeted advertising. Proposals to strengthen data protection remedies that may be accessed by users are likely. There will also probably be a lot of back and forth debate between regulators, commercial organisations, data protection authorities and individual Internet users, both at the European stage and at national levels. Users must once again consider the crucial question: what level of privacy is it reasonable to expect in the modern online environment. McNealy's recent remark that 'You have zero privacy. Get over it [12] seems to be more than a little premature. The current legal developments in Europe and elsewhere indicate that the opposite appears to be true: protecting privacy is a highly topical issue, and the lawmakers are having to run ever faster to keep up with the demands of online users for real protection against misuse of powers.

Bibliography

Primary Sources:

Legislation

1. Data Protection Directive 95/46/EC 1995
2. Product Liability Directive 85/374/EEC 1985

Cases

3. Lindqvist [2004] C-101/01

Secondary Sources:

Books

4. L. Edwards, and I. Brown, 'In Harboring data: Information security, law and the corporation', Data control and social networking: irreconcilable ideas (Stanford University Press 2009), p. 202–227.

Articles

5. Rebecca Wong, 'The Data Protection Directive 95/46/EC: Idealism and Realism', International Review of Law', (2012) Computers & Technology
6. Peter Fitzgerald 'Hidden Dangers in the E-Commerce Data Mine: Governmental Customer and Trading Partner Screening Requirements', (2001) The International Lawyer
7. Rebecca Wong, 'Data protection online: Alternative approaches to sensitive data', Journal of International Commercial Law and Technology (2007), 9 (16)

Online journals

8. K. McCullagh, 'Data sensitivity: resolving the conundrum', Journal of International Commercial Law and Technology (2007) 2 (4) <http://usir.salford.ac.uk/2745/1/32-126-1-PB.pdf> accessed 5 June 2016
9. R. Cellan-Jones, 'Irish privacy watchdog calls for Facebook changes' (BBC

News, 8 March 2012) http://www.bbc.co.uk/news/technology-16289426 accessed 5 June 2016

10. W. Hon, C. Millard, and I. Walden, 'Who is responsible for 'Personal Data' in Cloud

Computing', (2012) <http://www.cloudlegal.ccls.qmul.ac.uk/Research/researchpapers/45905.html> accessed 5 June 2016

11. S. Gibbs, 'EU agrees draft text of pan-European data privacy rules', The Guardian, 16 December 2015 < https://www.theguardian.com/technology/2015/dec/16/eu-agrees-draft-text-pan-european-data-privacy-rules> accessed 5 June 2016

12. S. McNealy, 'State of the Web: Who killed privacy? You Did?' Digital Trends (2012), <http://www.digitaltrends.com/opinion/state-of-the-web-who-killed-privacy/#:yhwFO6aGVLEAtA> accessed 5 June 2016

Working Papers

13. P. Seipel, 'Sweden. In Nordic data protection law' (2001)