MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY

VOLUME **16** | NUMBER **2** | FALL **2022** | ISSN **1802-5943**

PEER REVIEWED

CONTENTS:

www.mujlt.law.muni.cz

Masaryk University Journal of Law and Technology
issued by Institute of Law and Technology
Faculty of Law, Masaryk University
www.mujlt.law.muni.cz

Official Partner (Czech Republic)
ROWAN LEGAL, advokátní kancelář s.r.o. (www.rowanlegal.com/cz/)
Na Pankráci 127, 14000 Praha 4

Subscriptions, Enquiries, Permissions
Institute of Law and Technology, Faculty of Law, MU (cyber.law.muni.cz)

listed in HeinOnline (www.heinonline.org)
listed in Scopus (www.scopus.com)
reg. no. MK ČR E 17653

MASARYK UNIVERSITY JOURNAL OF
LAW AND TECHNOLOGY

VOLUME **16** | NUMBER **2** | FALL **2022**

LIST OF ARTICLES

DOI 10.5817/MUJLT2022-2-1

INTERNATIONAL JURISDICTION IN CROSS-BORDER INFRINGEMENT OF PERSONALITY RIGHTS IN THE EUROPEAN UNION

by

ANABELA SUSANA DE SOUSA GONÇALVES*

The legal provision applicable to determine the jurisdiction to decide claims regarding the cross-border infringement of personality rights is Article 7, Section 2, of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels Ia). This legal provision establishes the jurisdiction in non-contractual matters of the court of the place where the harmful event occurred or may occur. Called to interpret the concept of place where the harmful event occurred, the Court of Justice of the European Union (ECJ) was forced to make an interpretative effort in case of online infringement of personality rights, because the information that is placed online can be accessed in any country. The offences that occur on the Internet can have a global reach and cause damage with greater geographical extension and repercussions in the legal sphere of the victim, especially due to the geographical wide location of its users. The aim of this study is to highlight the latest trends of the ECJ regarding this topic.

KEY WORDS

Brussels Ia Regulation; international jurisdiction; online torts, delicts or quasi-delicts

1. INTRODUCTORY REMARKS

In the European Union (EU), the legal provision applicable to determine the jurisdiction to decide claims regarding the cross-border infringement of personality rights is Article 7, Section 2, of Regulation (EU) No 1215/2012 on jurisdiction and the recognition and enforcement of judgments in civil

* Professor of Law at the Law School of the University of Minho, Portugal; asgoncalves@direito.uminho.pt

and commercial matters (Brussels Ia). Article 7, Section 2, establishes jurisdiction in non-contractual matters to the court of the place where the harmful event occurred or may occur. Called to interpret the concept of place of occurrence of the harmful event, the Court of Justice of the European Union (ECJ) decided that the legal provision should have an autonomous interpretation from the substantive law of the Member States, taking into account the system and objectives of the Regulation[1]. To this extend, the ECJ decided that the place where the harmful event occurred or could occur simultaneously comprehends the place of the event, as also the place of the damage.

However, the online infringement of personality rights forced the ECJ to make a new interpretative effort, because the information that is placed online can be accessed in any country. Subsequently, the offences that take place on the Internet can have a worldwide reach and can cause damage with a larger geographical dimension and higher repercussions in the legal sphere of the victim, especially due to the geographical dissemination of the Internet users. The purpose of this study is to analyse the most recent cases of the ECJ regarding the cross-border infringement of personality rights.

2. BRUSSELS IA REGULATION

The Brussels Ia Regulation establishes a uniform system of legal provisions regarding international jurisdiction and a system of automatic recognition and enforcement of decisions in civil and commercial matters (Article 1). Brussels Ia is one of the main legal instruments of the policy of cooperation in civil matters, set in Article 81 of the Treaty on the Functioning of the European Union, that acts as a way of strengthening cooperation between judicial authorities of the Member States in order to simplify

[1] Judgment of 21 December 2021, Gtflix Tv v DR, C-251/20, ECLI:EU:C:2021:1036, paragraph 23; Judgment of 17 October 2017, Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB, C-194/16, EU:C:2017:766, paragraph 25; Judgment of 2011, eDate Advertising GmbH and Others v X and Société MGN LIMITED, C-509/09 and C-161/10, EU:C:2011:685, paragraph 38; Judgment of 16 July 2009, Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA2009, Case C-189/08, ECLI:EU:C:2009:475, paragraph 17; 2008, *Hassett and Doherty*, C-372/07; ECR I-7403, paragraph 17; Judgment of 23 April 2009, Draka NK Cables Ltd, AB Sandvik international, VO Sembodja BV and Parc Healthcare International Limited v Omnipol Ltd.2009, C-167/08, ECR I-3477, paragraph 19. About the autonomous interpretation of the Brussels Ia Regulation, taking into account its system and objectives, as well as the need to articulate the interpretation of the legal instruments regarding judicial cooperation in civil matters, see Gonçalves, A.S.S (2016) Cooperação judiciária em matéria civil e Direito Internacional Privado. In: Alessandra Silveira *et al.* (ed.) *Direito da União Europeia.* Coimbra: Almedina, pp. 330-291.

the cross-border enforcement of rights, through the principle of automatic recognition (Recital 3 of the Brussels Ia Regulation)[2].

Article 4, Section 1, is the general rule regarding international jurisdiction, that sets the jurisdiction of the court of the Member State of the defendant's domicile. In addition, Brussels Ia Regulation establishes a set of alternative jurisdictions for certain matters listed in Article 7. The attribution of alternative jurisdiction provided for in this legal provision is based on the principle of proximity, as these legal provisions are based in the existence of a particular close connection between the jurisdictions listed in the rule and the litigation. Therefore, this alternative jurisdiction is justified by the principle of trust, the protection of the legitimate expectations of the parties and the need of security and legal certainty, through the attribution of jurisdiction to a foreseeable jurisdiction, taking into account its proximity with the dispute. At the same time, some procedural advantages are also guaranteed, such as the efficient handling and organization of proceedings, the sound administration of justice and the production of evidence, with positive repercussions in fast the settlement of the dispute[3]. In the case of an alternative jurisdiction, the plaintiff, when bringing an action, can resort to the general rule of the court of the defendant's domicile (Article 4, Section 1) or to the special rule of Article 7. One of these special alternative jurisdictions concerns matters relating to tort, delict or quasi-delict, provided for in Section 2 of Article 7.

3. MATTERS RELATING TO TORT, DELICT OR QUASI-DELICT IN BRUSSELS IA REGULATION

Article 7, Section 2, gives jurisdiction in matters relating to tort, delict or quasi-delict to the courts of the place where the harmful event occurred or may occur. Called to interpret the concept of place where the harmful event occurred, the ECJ determined that this notion simultaneously covers

[2] For a more detailed view of this Regulation, see AAVV (2016) *ECPIL, European Commentaries of Private International Law, Brussels Ibis Regulation*. Ulrich Magnus, Pater Mankowski (ed.). Köln: OttoSchmidt; Gaudemet-Tallon, H. (2015) *Compétence et exécution des jugements en Europe, Matières civile et commerciale*. 5th ed. Paris: LGDJ; Gonçalves, A.S.S. (2014) A revisão do Regulamento Bruxelas I relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial. In: M.F. Monte, J.F. Rocha, J.A. Silva, E. Fernandez (ed.) *Estudos em Comemoração dos 20 Anos da Escola de Direito da Universidade do Minho*. Coimbra: Coimbra Editora, pp. 39-59.

[3] With more detail about the justification of alternative jurisdiction in Article 7, see Gaudemet-Tallon, H. (2015) Compétence et exécution des jugements en Europe, Matières civile et commerciale. 5th ed. Paris: LGDJ, pp. 195-196; Mankowski, P. (2016) Article 7. In: Ulrich Magnus, Pater Mankowski (ed.) *ECPIL, European Commentaries of Private International Law, Brussels Ibis Regulation*, Köln: OttoSchmidt, pp. 143-145.

both the place where the event giving rise to the damage occurred or the place where the damage occurred[4]. Also called upon to interpret the concept of place of occurrence of the damage, the ECJ decided that the damage relevant to the application of Article 7, Section 2, would only referred to the direct damage, that means the place where the direct results of the unlawful action or omission occurred[5].

This interpretation of the ECJ increased the number of courts available to the plaintiff, who, in addition to the general rule of the court where the defendant was domiciled, could resort to the court of the place of the event or to the court of the place of damage. However, the scope of jurisdiction of each of these courts is different, as the court of the place of damage would only have jurisdiction to decide on the damage that occurred in its territory. On the other hand, the court of the place of the event would have a broader jurisdiction, being able to assess all the consequences arising from that unlawful behaviour[6].

4. ONLINE TORTS, DELICTS OR QUASI-DELICTS

The occurrence of online torts, delicts or quasi-delicts forced the ECJ to make a new interpretative effort of Article 7, now taking into account the specific characteristics of the Internet. The Internet is a way of fast communication, where the information is globally disseminated and is accessible worldwide. The information that is placed online can be easily accessed in any country and the infringement of rights on the Internet can

[4] See this position, v.g., in Judgment of 30 November 1976, Handelskwekerij G. J. Bier B.V. v. Mines de Potasse d'Alsace S.A., C-21/76, ECLI:EU:C:1976:166. According with the ECJ jurisprudence, the interpretation given by the Court to the legal provisions of the 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters should be applied to the equivalent rules of Brussels I Regulation: see, v.g., Judgment of 16 July 2009, Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA2009, Case C 189/08, ECLI:EU:C:2009:475; Judgment of 1 October 2002, Verein für Konsumenteninformation v. Karl Heinz Henkel, C-167/00, ECLI:EU:C:2002:555; Judgment of 10 June 2004, Rudolf Kronhofer v. Marianne Maier and Others, C-168/02, ECLI:EU:C:2004:364.

[5] See, v.g., Judgment of 16 July 2009, Zuid-Chemie BV v Philippo's Mineralenfabriek NV/SA2009, Case C 189/08, ECLI:EU:C:2009:475; Judgment of 10 June 2004, Rudolf Kronhofer v. Marianne Maier and Others, C-168/02, ECLI:EU:C:2004:364; Judgment of 11 January 1990, Dumez France SA and Tracoba SARL v. Hessische Landesbank and others, C-220/88, ECLI:EU:C:1990:8; Judgment of 2011, eDate Advertising GmbH and Others v X and Société MGN LIMITED, C 509/09 and C 161/10, EU:C:2011:685, paragraph 41.

[6] About this interpretation, see Mankowski, P. (2016) Article 7. In: Ulrich Magnus, Pater Mankowski (ed.) *ECPIL, European Commentaries of Private International Law, Brussels Ibis Regulation*, Köln: OttoSchmidt, pp. 195-196; AAVV (2019) *Derecho Internacional Privado*, Vol. II. A.L. Calvo *Caravaca,* J. Carrascosa González (ed.). 14ª Ed. Granada: Comares, pp. 1062-1080; Virgós Soriano, M.; Garcimartín Alférez, F. (2007) *Derecho Procesal Civil Internacional, Litigación Internacional*. 2.ª Ed., Pamplona: Thomson Civitas, pp. 186-200; Salerno, F. (2006) *Giurisdizione ed Efficacia delle Decisioni Straniere nel Regolamento (CE) N. 44/2001 (La revisione della Convenzione di Bruxelles del 1980)*. 3.ª Ed. Padova: Cedam, pp. 150-166.

have a global reach. This means that the impact of the damage is broader, especially due to the wide geographic location of Internet users.

The characteristics of the Internet led the ECJ to adopt a *delict oriented approach* in the interpretation of the place where the damage occurred, in relation to online torts, delicts or quasi-delicts: that means, an interpretation that varies depending on the delict in question, taking into account the nature of the infringed right, the scope of geographic protection of that right and the analysis of the extent of the damage. The starting idea of the *delict oriented approach* is that the occurrence of damage in a given location depends on the condition that the right in question is protected in the territory of that State. Therefore, the *delict oriented approach* takes into account the area of geographic protection of the right, due to the need to identify the court best placed to assess the infringement of the right in question[7]. The ECJ has tested the delict oriented approach in several decisions regarding online torts, delicts or quasi-delicts. One example is the *Wintersteiger* case, in which it was at stake an infringement of an intellectual property right through the Internet, namely a registered trademark[8]; another example is the *Peter Pinckney* case, in which copyrights were infringed through content posted on a website[9]; the *Pez Hejduk* case regarded also an online copyright infringement[10]; the *Concurrence SARL* case was another example, that involved the online infringement of exclusive distribution rights[11].

Regarding the interpretation of the place of event in online torts, delicts or quasi-delicts, the ECJ has several decisions on the implementation of this concept in the cross-border infringement of personality rights.

5. THE CROSS-BORDER INFRINGEMENT OF PERSONALITY RIGHTS

On the *Shevill* case, the ECJ focused on the release through the press of a defamatory article published in several States. In this case, it was decided that the victim could file an action seeking compensation for all

[7] See with more detail about the delict oriented approach, Gonçalves, A.S.S. (2018) The application of the Brussels I Recast Regulation to wrongful activities online and the delict oriented approach. *European Journal of Law and Technology*, 9 (1), pp. 1-14.

[8] Judgment of 19 April 2012 2012, Wintersteiger AG v. Producuts 4USondermaschinenbau GmbH, C-523/10, ECLI:EU:C:2012:220.

[9] Judgment of 3 October 2013, Peter Pinckney v. KDG Mediatech AG, C-170/12, ECLI:EU:C:2013:635.

[10] Judgment of 22 January 2015, Pez Hejduk v. EnergieAgentur.NRW GmbH, C-441/13, ECLI:EU:C:2015:28.

[11] Judgment of 21 December 2016, Concurrence SARL v. Samsung Electronics France SAS, Amazon Services Europe Sàrl, C-618/15, ECLI:EU:C:2016:976.

the damages suffered in the place of the causal event, which would be the place of the establishment of the publisher, as this was the place where the unlawful act occurred: "that is the place where the harmful event originated and from which the libel was issued and put into circulation"[12]. As for the place where the damage occurred, the court ruled that in the case of cross-border libel through the press "the injury caused by a defamatory publication to the honour, reputation and good name of a natural or legal person occurs in the places where the publication is distributed, when the victim is known in those places"[13]. Therefore, it was considered that the courts of the State in which the publication was published and where the victim claims to have suffered an attack to his reputation would also have jurisdiction, as a court of the occurrence of the damage, with the specificity that these latter courts could only judge the damages occurring in the territory of that State[14]. This position is known as the mosaic approach (*Mosaikbetrachtung*), since potentially the victim can bring an action in the court of the place where each one of the damages occurred, and that court, in turn, can only decide the damages that occurred in its own territory[15].

On the eDate case, the ECJ again analysed a situation of transnational infringement of personality rights, however, the disclosure of harmful content was done through the Internet. In this case, the court recognized the specificity of the Internet, as, due to its characteristics and its worldwide reach, the impact of harmful content that was posted online on an individual's personality rights is greater and, consequently, is the scale of the damages that can produce[16]. Therefore, the ECJ maintained the position that the victim could appeal to the court of the causal event – in this case, the place of establishment of the content editor, for compensation for all damages. However, it could also bring an action in each of the Member States where the damage occurred, although in that case these courts would only have jurisdiction to rule on the damage that occurred in their territory. In addition, in the case of an online infringement,

[12] Judgment of 7 March 1995, Fiona Shevill, Ixora Trading INC., Chequepoint SARL e Chequepoint International LTD v. Presse Alliance SA., C-68/93, ECLI:EU:C:1995:61, paragraph 24.

[13] *Op cit*, paragraph 29.

[14] *Op cit*, paragraph 30 e 33.

[15] On scattered damage and the mosaic approach, *v.* Gonçalves, A.S.S. (2014) The application of the general rule of the Rome II Regulation on the internet torts. *Masaryk University Journal of Law and Technology*, 8 (1), pp. 64-66.

[16] Judgment of 2011, eDate Advertising GmbH and Others v X and Société MGN LIMITED, C 509/09 and C 161/10, EU:C:2011:685, paragraph 41.

the Court decided that the damage would occur in each of the States in whose territory the content placed online is or was accessible[17] and where the injured party claims that his reputation has been harmed[18].

Nevertheless, the ECJ was sensitive to the fact that Internet users are spread all over the world and that the content that is placed online can potentially be accessed in any State, which increases the impact of the damage. It also considered that "it is not always possible, on a technical level, to quantify that distribution with certainty and accuracy in relation to a particular Member State or, therefore, to assess the damage caused exclusively within that Member State"[19]. Taking into account the severity, the geographical extent of the damage and the difficulty of locating it in only one State, the ECJ considered that the court of the place where is the centre of interests of the victim, would have jurisdiction over all the damages[20]. The victim's centre of interests would be the place where the damage to the person's reputation would be greatest and would generally correspond to the place of his/her habitual residence[21]. However, the place of the centre of interests could also materialize in the place where the victim pursues his/her professional activity, if the person has a particularly close relationship with that State[22]. The jurisdiction of the court of the place where is based the centre of interests of the victim is justified, by the ECJ, in accordance with the principle of proximity and predictability underlying the rules of international jurisdiction, as the publisher of the wrongful content is in a position to know where is the centre of interests of the person who claims that is rights have been infringed. Furthermore, the possibility for this court to decide the totality of the damage is justified on the grounds of the sound administration of justice[23].

---

17 Note that victim is considered the direct victim of the damage. For further developments regarding this notion, see Gonçalves, A.S.S. (2013) *Da Responsabilidade Extracontratual em Direito Internacional Privado, A Mudança de Paradigma*. Coimbra: Almedina, pp. 374-380 and p. 406.

18 Judgment of 2011, eDate Advertising GmbH and Others v X and Société MGN LIMITED, C 509/09 and C 161/10, EU:C:2011:685, paragraph 42.

19 *Op cit*, paragraph 46.

20 *Op cit*, paragraph 48.

21 *Op cit*, paragraph 49.

22 *Ibid*.

23 *Op cit*, paragraph 48.

6. THE BOLAGSUPPLYSNINGEN CASE

On the Bolagsupplysningen decision, the ECJ was called again to interpret of the concept of place where the harmful event occurred, in cross-border infringement of personality rights through the Internet, in a case where a natural person and a legal person invoked the infringement of personality rights by the publication of incorrect information on a webpage and for not eliminating negative comments about them. The victims asked for the rectification of the information, the suppression of comments and a compensation for the damages suffered as a result of that publication.

In this case, the court restates the place of the victim's centre of interests "as the place in which a court can best assess the actual impact of the publication on the internet and its harmful nature"[24], and restates that this court should decide about all the damages suffered in the name of the sound administration of justice[25]. Once again, it is emphasized that this interpretation allows for the predictability of the rules of jurisdiction and legal certainty, making it easy for the plaintiff and the defendant to identify the forum[26]. The truth is that the centre of the activities of the person is: the place most identifiable with the person; where the person´s reputation is more deep-rooted and where he/she is interested in preserving it; where the greatest economic repercussions of the damage occur on the activity of the person, in case of damage to its reputation. This is clear in the Bolagsupplysningen case, where it is claimed that the information that Svensk Handel (the defendant and a company incorporated under Swedish law) placed on its website accusing Bolagsupplysningen of carrying out acts of fraud and deceit swindling, as well as the 1000 comments in the webpage that followed that publication, paralyzed the company's economic activity in Sweden (the main place of its activity), causing daily material losses.

As for the centre of interest of one of the claimants, Ilsjan, it is restated that, in the case of natural persons, this generally corresponds to their habitual residence, even though it may correspond to the place of exercise of their professional activity, if there is a close connection with that State[27]. Therefore, Estonia would be the place of Ilsjan's centre of interests, her habitual residence, and the Estonian court could assess the totality

[24] Judgment of 17 October 2017, Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB, C 194/16, EU:C:2017:766, paragraph 37.

[25] *Op cit*, paragraph 38.

[26] *Op cit*, paragraph 35.

[27] *Ibid*.

of the damages suffered. In this case, when the centre of interests coincides with the victim's habitual residence, a forum actoris is created and the protection of the victim is enhanced, since jurisdiction is given to the court that is closest to the victim[28].

In relation to the Bolagsupplysningen company, the other claimant and a legal person with commercial activity, the court decided that the place where the reputation of that person is most established should be searched, and should correspond to the place where the essential part of its economic activity is carried out, which may or may not coincide with the place of its registered office depending on the circumstances. However, in a situation, as in the case, where the registered office of the legal person is located in a Member State (Estonia), but most of its activities are carried out in another Member State (Sweden), the damage to the person's reputation is felt most in the latter[29]. Therefore, the Sweden courts (the State where were concentrated of the economic activities of the society and where society has established its reputation) would be the closest to decide the infringement of the right at stake. This is so, because the infringement of the company's reputation "is the publication of information and comments that are allegedly incorrect or defamatory on a professional site managed in the Member State in which the relevant legal person carries out the main part of its activities and that are, bearing in mind the language in which they are written, intended, for the most part, to be understood by people living in that Member State"[30]. Sweden will be considered the place where the damage to the victim's reputation occurred and it will assume jurisdiction as its centre of interests.

The ECJ also specified the concept of place of damage, taking into account its nature. The claimants asked for the rectification of incorrect information on the publication about them placed on the website and the elimination of comments related to them, published in the discussion forum. The ECJ decided that it would not be possible to resort to the courts of each of the Member States in whose territory the information is or was accessible in order to obtain the rectification of incorrect data or the removal of the comments[31]. According to the court, "in the light of the ubiquitous

[28] With the same opinion, see Vanleenhove, C. (2018) The European Court of Justice in Bolagsupplysningen: The Brussels I Recast Regulation's jurisdictional rules for online infringement of personality rights further clarified. *Computer Law & Security Review*, 34(3), p. 646.

[29] Judgment of 17 October 2017, Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB, C 194/16, EU:C:2017:766, paragraph 41.

[30] *Op cit*, paragraph 42.

[31] *Ibid.*

nature of the information and content placed online on a website and the fact that the scope of their distribution is, in principle, universal (…), an application for the rectification of the former and the removal of the latter is a single and indivisible application and can, consequently, only be made before a court with jurisdiction to rule on the entirety of an application for compensation for damage", as decided in the Shevill and eDate case[32]. In other words, the ECJ considered that the damage at skate (rectification of incorrect information and the elimination of the comments) was not geographically divisible. Consequently, it was not possible to resort, in this case, to the place of damage.

7. THE GTFLIX TV CASE

The recent Gtflix Tv case[33] helps to clarify the position taken by the ECJ in the Bolagsupplysningen decision. Gtflix Tv has its seat and centre of interest in the Czech Republic, where it produces and distributes, through the internet, adult audio-visual content. DR is a director, producer and distributor of films of the same type, marketed on websites hosted in Hungary, country where he has his domicile. Gtflix Tv claims that DR made defamatory comments about it on websites and forums and decides to bring an action against him asking: to cease all acts of belittling towards Gtflix Tv and to publish a legal notice in French and English on each of the internet forums; to consent in Gtflix Tv to post a comment on those forums; to pay Gtflix Tv a compensation for economic and non-material damages. In this case, the distinction between the different types of damages and how their nature affects the court jurisdiction becomes clear.

The action was brought before the French courts, as the courts of the place of the damage, and the doubt that was posed before the ECJ regarded the jurisdiction of the French courts, according with Article 7, Section 2. The ECJ restated that the victim can bring an action: for all the damages, before the place of the event giving rise to damages (place in which the publisher of that content is established); for all the damages, before the place of the victims centre of interests; before the courts of each Member State in which the content placed online is or has been accessible, as place of damage, but only regarding the damage occurred in that Member State[34].

[32] *Op cit*, paragraph 49.
[33] Judgment of 21 December 2021, Gtflix Tv v DR, C 251/20, ECLI:EU:C:2021:1036.
[34] *Op cit*, paragraph 30.

However, clarifying the Bolagsupplysningen decision, the ECJ states that an application for the rectification and the removal of information that is placed online is a single and indivisible application and can only be brought before a court that has jurisdiction to decide the totality of the damages, because due to the nature of the internet the spreading of a content placed online is universal[35]. Therefore, only the court of the event or the court of the centre of interest could decide this claim. On the other hand, regarding the compensation in respect of the damages resulting from the placement of the content online, the court ruled that the victim can ask compensation for all the damages, resorting to the referred courts, or only for a part of those damages. In this last case, the victim can bring an action for partial compensation in each Member State where the damage occurred, as long as those comments are or were accessible in that Member State[36]. These courts will only have jurisdiction to rule on the damage occurred in its territory.

8. THE MITTELBAYERISCHER CASE

The Mittelbayerischer case has the specificity that the person that claims the infringement of his personality rights by the content placed online on the Mittelbayerischer website is not directly or indirectly referred on that content. SM was a Polish national, residing in Poland, and was a prisoner in the extermination camp at Auschwitz during the Second World War. Mittelbayerischer Verlag is a German company, that publishes an online newspaper in its website, in German, but accessible from other countries. SM claims that his personality rights were infringed, namely his national identity and dignity, with an expression published by the defendant that stated that the Treblinka camp, situated in Poland, was a Nazi extermination camp. Latter, this expression was substituted by German Nazi extermination camp of Treblinka, situated in occupied Poland[37]. The question posed to the ECJ was if the Polish courts could have jurisdiction according with Article 7, Section 2, as the courts of the place where the claimant has his centre of interests.

The ECJ invoked the foreseeability and legal certainty of rules of jurisdiction to justify that a person that is not mentioned or indirectly identified by a content put online cannot resort to the courts of its centre

35 *Op cit*, paragraph 32.

36 *Op cit*, paragraph 43.

37 Judgment of 17 June 2021, Mittelbayerischer Verlag KG v SM, Case C-800/19, ECLI:EU:C:2021:489, paragraph 7-12.

of interest, because the defendant could not "reasonably foresee being sued before those courts, since they are not, at the time when they place content online on the internet, in a position to know the centres of interests of persons who are not in any way referred to in that content"[38]. Another interpretation would multiply the courts that would have jurisdiction to decide the entire damage, not taking into consideration that Article 7, Section 2, is an exception to the general rule of Article 4; should be interpreted strictly; and to be applicable, there should be a particular close connection between the litigation and the courts set in the legal provision, to guarantee legal certainty and the predictability of the forum[39]. That close connection cannot lay "on exclusively subjective factors, relating solely to the individual sensitivity of that person, but on objective and verifiable elements which make it possible to identify, directly or indirectly, that person as an individual"[40]. The fact that SM is a part of an identifiable group referred in the content placed online is not enough, because it does not translate into closer connection between the place of its centre of interests and the dispute[41]. Consequently, the person that claims that his personality rights were infringed by a content place online can only rely on the courts of his centre of interests "if that content contains objective and verifiable elements which make it possible to identify, directly or indirectly, that person as an individual"[42].

9. GLOBAL PERSPECTIVE

In Mittelbayerischer case, the ECJ decides that the connecting factors of the jurisdiction rules should be established with the direct victim of the tortious action. This position is in line with the notions established by Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II). The notion of the person sustaining damage of Article 4, Section 2, of the Rome II Regulation must be interpreted as the direct victim of the damage, which may not coincide with the person seeking compensation. This is the most appropriate interpretation, because it is according with the notion of damage established in Article 4, Section 1, of the same Regulation, which gives relevance to the direct damage[43]. This legal provision of the Rome II Regulation, refers to the place where

38 *Op cit*, paragraph 38.
39 *Op cit*, paragraph 40.
40 *Op cit*, paragraph 42.
41 *Op cit*, paragraph 44.
42 *Op cit*, paragraph 46.

the direct damage occurs, that means that the tort/delict will be govern by the law of the place where the direct results of the event occurred, following the notion of direct damage set by jurisprudence of the ECJ, regarding the jurisdiction rule of Article 7, Section 2, of Brussels Ia Regulation[44]. So, one can conclude that in the Mittelbayerischer decision there is consistency between the notions set in Brussels Ia and Rome II Regulations, following Recital 7 of Rome II Regulation, that establishes the consistency between the instruments dealing with jurisdiction and the applicable law [45].

This interpretation also avoids the multiplication of forums, and takes under consideration the objectives of the special rules of Article 7: close connection between the dispute and the court; legal security; and predictability of the defendant about the jurisdiction. Another interpretation would create jurisdictions with weak connection with the dispute and would make impossible for the defendant to foresee the jurisdiction, since the internet has a global reach and the claimant could have his centre of interests in any Member State. As set in Recital 16 of the Brussels Ia Regulation, the predictability of the jurisdiction is particularly important in violations of rights relating to personality, including defamation.

The Bolagsupplysningen and Gtflix Tv cases follows the delict oriented approach already stated in other cases of delicts on the internet: when online activities cause damages, the place where the damage occurs varies according to the nature of the right infringed and the scope of geographical protection of that right, which implies an analysis of the infringement,

---

[43] With the same position, see Dickinson, A. (2010) *The Rome II Regulation, The Law Applicable to Non-Contractual Obligations*. Oxford: Oxford Publishing Press, p. 339; Gonçalves, A.S.S. (2013) *Da Responsabilidade Extracontratual em Direito Internacional Privado, A Mudança de Paradigma*. Coimbra: Almedina, p. 406; Von Hein, H. (2011) Article 4 General Rule. In: Gralf Peter Calliess (ed.) *Rome Regulations, Commentary on the European Rules on the Conflict of Law*. The Netherlands: Workers Kluwer, p. 416; Magnus, U. (2019) Article 4 General Rule. In: Ulrich Magnus, Pater Mankowski (ed.) *ECPIL, European Commentaries of Private International Law, Rome II Regulation*, Köln: OttoSchmidt, pp. 179-180.

[44] Judgment of 11 January 1990, Dumez France SA and Tracoba SARL v. Hessische Landesbank and others, C-220/88, ECLI:EU:C:1990:8; Judgment of 19 September 1995, Antonio Marinari v Lloyds Bank plc and Zubaidi Trading Company, Case C-364/93, ECLI:EU:C:1995:289; Judgment of 10 June 2004, Rudolf Kronhofer v. Marianne Maier and Others, C-168/02, ECLI:EU:C:2004:364; Judgment of 27 October 1998, Réunion européenne SA and Others v Spliethoff's Bevrachtingskantoor BV and the Master of the vessel Alblasgracht V002, Case C-51/97, ECLI:EU:C:1998:509.

[45] According with the European Commission, the Brussels I, Rome II and the Rome I Regulations form an inseparable group of rules, setting the legal framework of European Union private international law in matters of contractual and non-contractual obligations in civil and commercial matters: European Commission. (2005) *Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations* (Rome I). Brussels: COM/2005/0650 final - COD 2005/0261, p. 2.

the nature of the right, and its geographical area of protection[46]. However, in cases of online infringement of personality rights, one can question the appropriateness of scattering the damage, giving jurisdiction to each of the Member States where the content that was placed online can be assessed. The ubiquitous nature of the Internet and the spreading of its users allows worldwide dissemination of the content placed online. So, in online infringement of personality rights it can be difficult on a technical level to distribute the damage through several countries and for the court to assess the existence and extension of the damage in its territory. Besides, although the ECJ does not agree[47], it is undeniable the link of dependence between the application for the rectification and the removal of content placed online and the application for compensation in respect of the damages resulting from that placement. It would be quite strange if, regarding the same situation, one court ruled that there was no infringement of personality rights, refusing the rectification and the removal of content placed online, and another court would grant compensation for the damages occurred in its territory for the infringement of personality rights.

It is necessary to adapt the jurisprudence to the specificity of the internet when there is a violation of a personality right[48]. Consequently, foreseeability and legal certainty, and the need of consistency would require the ECJ to rethink its jurisprudence on online infringement of personality rights and to give jurisdiction to the court that is able to assess the totality of the damages, respecting the closer connection between the court and the entire dispute. That would mean to restrict jurisdiction to the place of the victim's centre of interests (as the place where the damage to the reputation of the victim occurred) or to the place of the event, eliminating the jurisdiction of the place of the damage and the mosaic

[46] For a more in-depth understanding, see Gonçalves, A.S.S. (2018) The application of the Brussels I Recast Regulation to wrongful activities online and the delict oriented approach. *European Journal of Law and Technology*, 9 (1), pp. 1-14.

[47] Judgment of 21 December 2021, Gtflix Tv v DR, C 251/20, ECLI:EU:C:2021:1036, paragraph 36.

[48] Underlining the importance of adapting the rules of the Brussels Ia Regulation to offences that occur on the Internet, v. Calvo Caravaca, A.L., Carrascoza González, J. (2001) *Conflictos de leyes y conflictos de jurisdicción en internet*. Madrid: Colex.; Feraci, O. (2012) Diffamazione internazionale a mezzo di Internet: quale foro competente? Alcune considerazioni sulla sentenza 'eDate'. *Rivista di Diritto Internazionale*. 95 (2), pp. 461-469; Zarra, G. (2015) Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo internet. *Rivista di Diritto Internazionale*. 98 (4), pp. 1234-1262; Lorente Martínez, I. (2012) Lugar del hecho dañoso y obligaciones extracontractuales. La sentencia del TJUE de 25 octubre 2011 y el coste de la litigación internacional en Internet. *Cuadernos de Derecho Transnacional*. Vol. 4(1), pp. 277-301; Cedeño Hernán, M. (2021) La tutela transfronteriza de los derechos de la personalidad en la Unión Europea. *Cuadernos de Derecho Transnacional*. 13(1), pp. 110-133.

approach. This would be more in line with the nature of the online infringement of personality rights and the characteristics of the Internet, as a global instrument of spreading information. It would also allow the consistency in the judgment of different claims regarding the same situation, avoiding contradictory decisions. Moreover, it would make it easier the judgment of these cases and would contribute to the sound administration of justice and the efficiency in the production of proof, because on a territorial level, it is not easy to locate the online infringement of personality rights through several Member States and to calculate the compensation of partial damages in each Member State. Finally, to resort to one court to decide all claims regarding the same situation (the court of the place of the event or the court of the centre of interests of the victim) would be in the best interest of the victim, that would have a more comprehensive decision.

10. FINAL REMARKS

The aim of this study is to highlight the latest trends of the ECJ regarding international jurisdiction in cross-border infringement of personality rights in the European Union, which is important to the debate that is starting about the need to introduce some changes in the Brussels Ia Regulation[49].

From the analysis of the recent decisions of the ECJ, it is clear that there is, by this time, a settled case law regarding the court of the place of the victim's centre of interests regarding the cross-border infringement of personality rights. The international jurisdiction of the victim's centre of interests began to be outlined in the eDate decision and has been reaffirmed over the years in the various ECJ decisions, only regarding cross-border infringement of personality right, and is not applicable to infringement of other torts or delicts. Consequently, it should be considered in a future recast of Brussels Ia the distinction of the infringement of personality rights from other torts and delicts, taking into account the specificity of the first. In addition, the legal provision regarding the infringement of personality rights should finally take to the Brussels Ia Regulation wording the criteria of the victim´s centre of interest that was developed by the ECJ. As demonstrated, this criterion has advantages to determine the jurisdiction in cross-border infringement of personality rights: close connection between the dispute and the court;

[49] Defending the need to reform Brussels Ia Regulation and with some suggestions, see Hess, B. (2022) La reforma del Reglamento Bruselas I bis. Posibilidades y perspectivas. *Cuadernos de Derecho Transnacional*, 14(1), pp. 10-24.

legal security; predictability of the defendant about the jurisdiction; efficient handling and organization of proceedings; sound administration of justice and production of evidence; with positive consequences in fast the settlement of the dispute.

From the analysis of the recent decisions of the ECJ, it also results that the place of the damage and the mosaic approach are not the most adequate criteria to be applied to online infringement of personality rights and that it should be given jurisdiction to the court that can assess the totality of the damages, respecting the closer connection between the court and the entire dispute[50]. As demonstrated, it endangers the sound administration of justice, the predictability of the rules of jurisdiction and the consistency in the judgment of different claims regarding the same situation. A future reform of the Brussels Ia Regulation should consider, whether this ECJ jurisprudence is in line with the principles that underlie the alternative jurisdiction of Article 7, Section 2, the specificities of cross-border infringement of personality rights, and the need of the victim to search for redress in the most appropriate jurisdiction to protect his/her rights relating to personality, including defamation.

LIST OF REFERENCES

[1] AAVV (2016) *ECPIL, European Commentaries of Private International Law, Brussels Ibis Regulation*. Ulrich Magnus, Pater Mankowski (ed.). Köln: OttoSchmidt.

[2] AAVV (2019) *Derecho Internacional Privado*, Vol. II. A.L. Calvo Caravaca, J. Carrascosa González (ed.). 14ª Ed. Granada: Comares.

[3] Calvo Caravaca, A.L.; Carrascoza González, J. (2001) *Conflictos de leyes y conflictos de jurisdicción en internet*. Madrid: Colex.

[4] Cedeño Hernán, M. (2021) La tutela transfronteriza de los derechos de la personalidad en la Unión Europea. *Cuadernos de Derecho Transnacional*. 13(1), pp. 110-133.

[5] Dickinson, A. (2010) *The Rome II Regulation, The Law Applicable to Non-Contractual Obligations*. Oxford: Oxford Publishing Press.

[6] European Commission. (2005) *Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)*. Brussels: COM/2005/0650 final - COD 2005/0261.

[50] With, the same opinion considering that the place of damage and the mosaic approach should be limited to the infringements of printed publications: Hess, B. (2022) La reforma del Reglamento Bruselas I bis. Posibilidades y perspectivas. Cuadernos de Derecho Transnacional, 14(1), p. 18.

[7] Feraci, O. (2012) Diffamazione internazionale a mezzo di Internet: quale foro competente? Alcune considerazioni sulla sentenza 'eDate'. *Rivista di Diritto Internazionale*. 95 (2), pp. 461-469.

[8] Gaudemet-Tallon, H. (2015*) Compétence et exécution des jugements en Europe, Matières civile et commerciale*. 5th ed. Paris: LGDJ.

[9] Gonçalves, A.S.S. (2013) *Da Responsabilidade Extracontratual em Direito Internacional Privado, A Mudança de Paradigma*. Coimbra: Almedina.

[10] Gonçalves, A.S.S. (2014) A revisão do Regulamento Bruxelas I relativo à competên-cia judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial. In: M.F. Monte, J.F. Rocha, J.A. Silva, E. Fernandez (ed.) *Estudos em Comemoração dos 20 Anos da Es-cola de Direito da Universidade do Minho*. Coimbra: Coimbra Editora, pp. 39-59.

[11] Gonçalves, A.S.S (2016) Cooperação judiciária em matéria civil e Direito Internacional Privado. In: Alessandra Silveira et al. (ed.) *Direito da União Europeia*. Coimbra: Almedina, pp. 330-291.

[12] Gonçalves, a.s.s. (2018) The application of the Brussels I Recast Regulation to wrongful activi-ties online and the delict oriented approach. *European Journal of Law and Technology*, 9 (1), pp. 1-14.

[13] Von Hein, H. (2011) Article 4 General Rule. In: Gralf Peter Calliess (ed.) *Rome Regulations, Commentary on the European Rules on the Conflict of Law*. The Netherlands: Workers Kluwer, p. 406-416.

[14] Hess, B. (2022) La reforma del Reglamento Bruselas I bis. Posibilidades y perspectivas. *Cuadernos de Derecho Transnacional*, 14(1), pp. 10-24.

[15] Lorente Martínez, I. (2012) Lugar del hecho dañoso y obligaciones extracontractuales. La sentencia del TJUE de 25 octubre 2011 y el coste de la litigación internacional en Internet. *Cuadernos de Derecho Transnacional*. Vol. 4(1), pp. 277-301.

[16] Magnus, U. (2019) Article 4 General Rule. In: Ulrich Magnus, Pater Mankowski (ed.) *ECPIL, European Commentaries of Private International Law, Rome II Regulation*. Köln: OttoSchmidt, pp. 170-188.

[17] Mankowski, P. (2016) Article 7. In: Ulrich Mag-nus, Pater Mankowski (ed.) *ECPIL, European Commentaries of Private International Law, Brussels Ibis Regulation*. Köln: OttoSchmidt, pp. 133-145.

[18] Salerno, f. (2006) *Guirisdizione ed Efficacia delle Decisioni Straniere nel Regolamento (CE) N. 44/2001 (La revisione della Convenzione di Bruxelles del 1980)*. 3.ª Ed. Padova: Cedam.

[19] Vanleenhove, C. (2018) The European Court of Justice in Bolagsupplysningen: The Brussels I Recast Regulation's jurisdictional rules for online infringement of personality rights further clarified. *Computer Law & Security Review*, 34(3), pp. 640-646.

[20] Virgós Soriano, M.; Garcimartín Alfé-Rez, F. (2007) *Derecho Procesal Civil Internacional, Litigación Internacional*. 2.ª Ed., Pamplona: Thomson Civitas.

[21] Zarra, G. (2015) Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo internet. *Rivista di Diritto Internazionale*. 98 (4), pp. 1234-1262.

DOI 10.5817/MUJLT2022-2-2

DISPUTE RESOLUTION MECHANISM FOR SMART CONTRACTS

by

MARINA KASATKINA*

Disputes regarding smart contracts are inevitable, and parties will need means for dealing with smart contract issues. This article highlights the need for dispute resolution mechanisms for smart contracts. The author provides analysis of the possible mechanisms to solve disputes arising from smart contracts, namely dispute resolution by traditional arbitration institutions and blockchain arbitration. Article acknowledges the benefits and challenges of both mechanisms. In the light of this, the author concludes about instituting a hybrid approach aimed at resolving disputes that will not stymie efficiencies of smart contracts.

KEY WORDS

Smart Contracts, Blockchain Technology, Digital Disputes, Dispute Resolution Mechanism, Off-chain, On-chain.

1. INTRODUCTION

With the rapid development of new technologies occurring during the fourth industrial revolution, new types of disputes with significant specifics are gradually beginning to form. A special category among them belongs to disputes arising from smart contracts based on blockchain technology. Smart contracts are not really "contracts" in the true sense of the word, understood by most as negotiated terms in an arms-length transaction (or "meeting of the minds").[1] Enforcement is automatic, and the code is immutable. Therefore, smart contracts on the blockchain

* m.kasatkina@maastrichtuniversity.nl, Ph.D. candidate, Maastricht University, Netherlands

1 Schmitz, A. J. and Rule, C. (2019) Online Dispute Resolution for Smart Contracts. *Journal of Dispute Resolution. University of Missouri School of Law Legal Studies Research Paper,* 2019 (11). Available from: https://ssrn.com/abstract=3410450 [Accessed 12 April 2022].

present a different set of challenges due to the inflexibility of the code-based executions.

It has to be noted that there is a close interaction between the real world and the software transaction world. Smart contracts inherently interfere with real-world people or institutions, which would result in legal issues due to the nature of our societies.[2] For the reason that virtual experiences lead to specific actions in the real world, disputes are inevitable. Possible scenarios in which disputes may arise include changing of circumstances, creating undesirable results for one party, absence of legal capacity to enter into the smart contract. Smart contracts may not be accurately coded to encompass the parties' original intentions. Moreover, coders may be sued for liability as a result of inaccurate smart contracts, or hackers may be prosecuted for interfering with or manipulating smart contracts.[3] In this respect, the potential need for dispute resolution mechanism is inevitable. But nowadays, there exist no well-defined system of rules applicable to smart contracts. All these aspects show that there is room for identifying dispute resolution mechanisms for smart contracts.

Generally speaking, there are two possible ways to resolve such disputes. According to the first approach, they are subject to review by traditional courts. The second approach assumes that arbitration institutions lend to resolve disputes arising out of smart contracts. They, in turn, are divided into two groups:

a) "off-chain" arbitration, meaning dispute resolution by traditional arbitration institutions guided by the usual rules;

b) "on-chain" arbitration that assumes to create innovative applications based on blockchain technology and designed to resolve disputes arising in a digital decentralized environment (blockchain arbitration).[4]

My focus in this article is on the possible mechanisms to solve disputes arising from smart contracts. I have two aims: first, to outline a framework for dispute resolution by traditional arbitration institutions and blockchain arbitration, and second, based on advantages and disadvantages of both

---

[2] Clément, M. (2019) Smart Contracts and the Courts. In: DiMatteo, L., Cannarsa, M. and Poncibò, C. (eds.) The *Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms.* Cambridge University Press, pp. 271–287.

[3] Zaslowsky, D. (2018) *What to Expect When Litigating Smart Contract Disputes.* [online] Available from: https://www.law360.com/articles/1028009/what-to-expect-when-litigating-smart-contract-disputes [Accessed 02 May 2022].

[4] International Chamber of Commerce (2018). *ICC Dispute Resolution Bulletin. Issue 1.* Available from: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/2018_12_13_icc_robots_arbitrator.pdf [Accessed 02 May 2022].

mechanisms I introduce a new hybrid approach to blockchain dispute resolution, that combines both on and off-blockchain components.

2. ANALYSIS OF THE POSSIBLE DISPUTE RESOLUTION MECHANISMS

The first question while considering dispute resolution mechanisms should be asked whether traditional courts could adjudicate disputes arising from smart contracts. In this respect, the following should be mentioned. Firstly, a smart contract is the code, which is understandable to programmers, not lawyers and judges. Courts may be substantially challenged in interpreting smart contracts, written in a coded language, that is not understandable to a human observer. Furthermore, a court could not intervene to prevent or reverse an automatic contract, since the execution of smart contracts does not allow for modifications.[5] As James Grimmelmann notes,

> *"…as long as the code does what it is supposed to and blockchain nodes achieve consensus, the intent and actions of one's counterpart do not matter; once triggered, the contract moves forward as defined at the time of its writing, regardless of either party's change in circumstances, misunderstandings, or otherwise."*[6]

In this regard, it is important to distinguish between two main models of smart contracts: external and internal.[7] External smart contracts are those that are governed by traditional, natural language contracts with the smart, code-driven part of the contract merely automating the performance of terms as appropriate (e.g. payment, shipment, etc.). If there is any disagreement between the parties, the traditional, non-code version of the contract prevails. An external smart contract must be clear about which version of the contract prevails in order to successfully put the natural-language terms first and foremost. However, when such clarity is lacking in multi-language contracts, the UNIDROIT Principles stipulate

---

[5] Rodrigues, U. (2018) Law and the Blockchain. *Iowa Law Review,* 104. Available from: https://ilr.law.uiowa.edu/print/volume-104-issue-2/law-and-the-blockchain/ [Accessed 02 May 2022].

[6] Grimmelmann, J. (2019) All Smart Contracts are Ambiguous. *Journal of Law & Innovation,* 2 (1). Available from: https://www.law.upenn.edu/live/files/9782-grimmelmann-all-smart-contracts-are-ambiguous [Accessed 02 May 2022].

[7] Chamber of Digital Commerce. (2018) *Smart Contracts: Is the Law Ready?* Available from: https://www.theblockchaintest.com/uploads/resources/CDC%20-%20Smart%20Contract-Is%20the%20Law%20Ready%20-%202018%20-%20Sep.pdf [Accessed 02 May 2022].

that preference should be given to the contract that was originally drawn up. Presumably, the same can apply to smart contracts; if the code was written first and the natural-language contract second, the code prevails. Inversely, one may say that code is not a "human" language of any kind and therefore should be interpreted as an appendix for the natural language contract, but not the main, binding part of any agreement. This approach may work in certain contexts, however, given that the code creates an outcome automatically, its interpretive value seems more relevant to the main body of most external smart contract.[8]

In the internal smart contracts, the code is supreme and any natural--language portion of the agreement is secondary. Therefore, while the natural-language portion of the contract may help courts understand the parties' intent, they will still have to interpret code to understand what consensus was reached. While this has been raised as a problem for courts wishing to exert power over smart contracts, the use of expert witnesses who can read and inform the court what the code "says", can quickly and easily remedy this issue (e.g. bringing a programmer to the stand to testify what the outcome of the code, as written, would be).[9] Thus, regardless of the specific type of smart contract, the inflexibility of code-based executions presents potential challenges.

Secondly, the anonymous nature of smart contracts and the fluidity of online identities make it difficult to determine the identities of the parties. The aforementioned anonymity gained by the use of public-key encrypted identities and VPNs. Nodes that contain the blockchain and all of its information are located all over the world. Transactions in the blockchain are fully networked and present only in cyberspace. The nodes hold imperfect partial copies of the blockchain; no particular node holds the entire blockchain.[10] And the decentralized nature of smart contracts prevents courts from establishing jurisdiction and determining the choice of law based on traditional rules.

For all of these reasons, it can be concluded that smart contract disputes should not be resolved by any national court. This leads to the demand for

---

[8] Sillanpaa, T. (2020) Freedom to (Smart) Contract: The Myth of Code and Blockchain Governance Law. *IALS Student Law Review,* 7 (2). Available from: https://journals.sas.ac.uk/lawreview/issue/view/582 [Accessed 02 May 2022].

[9] Ibid.

[10] Kaal, W. A. and Calcaterra, C. (2018) Crypto Transaction Dispute Resolution. *Business Lawyer*. Available from: http://dx.doi.org/10.2139/ssrn.2992962 [Accessed 05 May 2022].

resolving smart contract disputes with cross-jurisdictional, extra-legal, and efficient remedies.

Therefore, international arbitration presents a well-suited alternative for smart contract disputes as they have many common features, such as functioning in a decentralized manner, flexibility, confidentiality of proceedings. Nowadays, there exist two main approaches for dealing with smart contract issues, namely "on-chain" and "off-chain" arbitration.[11]

2.1 "OFF-CHAIN" ARBITRATION (DISPUTE RESOLUTION BY TRADITIONAL ARBITRATION INSTITUTIONS)

According to this approach, smart contracts can operate within the existing contract law framework, and disputes arising from them are subject to the arbitration institutions.[12] In this regard, a special arbitration center dealing with the resolution of digital disputes is being created or a specialized board in the existing arbitration institutions is being formed. Generally speaking, "off-chain" dispute resolution system could be characterized as a combination of traditional forms of dispute resolution process, lacking a mechanism for the automatic enforcement of the award.

For instance, on the 8th of November 2018 was opened the *Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce* (hereinafter "Court of Arbitration") which purpose is to resolve disputes related to digital technologies.[13] It is Europe's first and the world's second (after Japan) arbitral tribunal specializing in blockchain. Court of Arbitration applies the provisions of the Rules of the Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce (hereinafter "Rules").[14] According to paragraph 3 of the Rules, the Court of Arbitration has jurisdiction over a dispute if the parties conclude a written agreement (arbitration agreement) in the following forms:

---

[11] Szczudlik, K. (2019) *"On-chain" and "off-chain" arbitration: Using smart contracts to amicably resolve disputes.* [online] Available from: https://newtech.law/en/on-chain-and-off-chain-arbitration-using-smart-contracts-to-amicably-resolve disputes [Accessed 02 May 2022].

[12] De Filippi, P. and Wright A. (2018) *Blockchain and the Law: The Rule of Code.* Cambridge, Cambridge, MA: Harvard University Press, 300; Holden R. and Malani A. (2018) Can Blockchain Solve the Holdup Problem in Contracts? *University of Chicago Coase-Sandor Institute for Law & Economics. Working Paper,* 846.

[13] *The Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce.* [online] Available from: https:// blockchaincourt.org/ [Accessed 02 May 2022].

[14] The Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce (2019). The *Rules of the Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce.* Available from: https://blockchaincourt.org/wp-content/uploads/2019/07/The-Rules-of-the-Court-of-Arbitration-ENG.pdf [Accessed 04 May 2022].

a) a clause included in letters exchanged between the parties or declarations made by the parties by means of remote communication that enable the content of such declarations to be recorded

b) a reference made in a written agreement to a document containing a provision on submitting disputes to resolution by the Court of Arbitration. The dispute resolution process is carried out according to the standard arbitration procedure with certain exceptions. Firstly, the number of arbitrators for resolution of the dispute could be 5 or 7 in contrast to "traditional" arbitration (paragraph 19 of the Rules), where the number of arbitrators is limited (1 or 3). Secondly, an award made by the Court of Arbitration shall be pronounced at the same hearing at which the trial is closed. When pronouncing the award, the presiding arbitrator shall state orally the main reasons upon which such award is based (paragraph 45 of the Rules). Whereas the traditional arbitration ends without the announcement of the decision, which is sent to the parties later.

This approach also includes the creation of specialized boards in the existing arbitration institutions. For example, in 2018, the *Arbitration center of the Russian Union of Industrialists and Entrepreneurs (RSPP)* announced the formation of a new *Panel on disputes in the digital economy*. The panel was created to resolve disputes arising from transactions involving automatic execution, including using information systems based on a distributed registry (blockchain); disputes arising from the issuance, accounting and circulation of digital rights and disputes over transactions made using and (or) in relation to digital financial assets.[15] Due to the absence of special rules, the proceedings on such disputes are conducted according to the Rules of the arbitration center at the RSPP 2018.[16]

The above-mentioned approach to the disputes arising from smart contracts is considered the mainstream view. Although in the legal literature it is often criticized.[17] Instead, it is proposed to create special methods of dispute resolution based on technology- blockchain arbitration.

---

[15] *Arbitraznyu zentr pri RSPP.* [online] Available from: https://arbitration-rspp.ru/about/structure/boards/digital-disputes/ [Accessed 04 May 2022].

[16] Ibid.

[17] Schmitz, A. and Rule C. (2019) Online Dispute Resolution for Smart Contracts. *Journal of Dispute Resolution,* 2, pp. 103–125.

2.2 "ON-CHAIN" ARBITRATION (BLOCKCHAIN ARBITRATION)

This group includes projects that provide for the creation of new mechanisms specifically designed to resolve disputes arising from smart contracts. "On-chain" arbitration contains solutions in which the equivalent of a traditional arbitration decision is automatically executed by a smart contract without the involvement of any third parties. For instance, this could be realized with the help of certain assets, which, upon the occurrence of a defined condition, are transferred from one party to the other.[18]

This approach contemplates smart contracts as distinct legal tools, rather than digital alternatives to traditional legal contracts. From this perspective, blockchain technologies and smart contracts may create new legal systems, or a new *Lex Cryptographia*.[19] Several characteristics of blockchain-based technologies and smart contracts, such as its anonymity, automatic execution, and tamper-resistance, mean that

> *"existing legal infrastructure cannot address legal challenges presented by crypto transaction disputes".*[20]

Instead, these disputes require a "distributed jurisdiction" created through a process of institutional innovations.

Currently, there exist more than 20 projects that use blockchain to automate dispute resolution. All these projects could be divided into two groups:

a) Special on-line arbitration (CodeLegit, Cryptonomica, Juris, Mattereum, SAMBA);

b) Crowdsourced dispute resolution (Aragon, BitCad, CrowdJury, Confideal, Jur, Kleros, Oath).

In this article, I examined the most noteworthy projects, which have already been tested by end users.

---

[18] Szczudlik, K. (2019) *"On-chain" and "off-chain" arbitration: Using smart contracts to amicably resolve disputes.* [online] Available from: https://newtech.law/en/on-chain-and-off-chain-arbitration-using-smart-contracts-to-amicably-resolve disputes [Accessed 02 May 2022].

[19] De Filippi, P. and Wright A. (2018) *Blockchain and the Law: The Rule of Code.* Cambridge, Cambridge, MA: Harvard University Press, 300.

[20] Kaal, W. A. and Calcaterra, C. (2018) Crypto Transaction Dispute Resolution. *Business Lawyer.* Available from: http://dx.doi.org/10.2139/ssrn.2992962 [Accessed 05 May 2022].

2.2.1 SPECIAL ON-LINE ARBITRATION

This group includes platforms that enable the creation of a special arbitration combining the advantages of international commercial arbitration and blockchain technology. They presume the automation of certain elements of the proceedings. However, the mechanism of their action is in many ways similar to international arbitration, as the rules of many such projects are based on the UNCITRAL Arbitration Rules. In this case, the decision made by the arbitrators is executed in the traditional way or is automatically executed with a smart contract.

For instance, a *Juris project* that presents a blockchain-based development system, operating on the basis of the Juris Protocol Mediation and Arbitration.[21] A prerequisite for considering a dispute is the existence of an arbitration agreement, integrated into a smart contract via a coded clause. In case of a dispute between the parties, a user initiates a protocol by filing a complaint (Formal Complaint). The system suspends further execution of the smart contract generation and notifies the other party about the dispute. After that, the following three procedures are possible:

1) Self Mediation – through which the parties get access to a number of tools, specially designed for self-regulation dispute resolution with the help of Self-Enforced Library Functions (or Self layer). These tools enable the execution of basic operations that alter the outcome of a smart contract implementation (such as contract cancellation and asset transfer). In the case of impossibility to resolve the dispute, parties could escalate to the second stage.

2) SNAP (Simple Neutral Arbitrator Poll) means the consideration of the dispute by independent arbitrators. Results of the voting are reported to the parties. Based on this information, the parties still may try to resolve the dispute by using Self layer or applying to the third tool.

3) PANEL (Juris Peremptory Agreement for Neutral Expert Litigation) is the analogue of traditional arbitration proceedings based on the UNCITRAL Arbitration Rules. The dispute is reviewed by three arbitrators selected on the basis of their reputation and compliance with the requirements specified by the parties while entering into the contract.

[21] Kerpelman, A. J. (2018) *Introducing the Juris Protocol: Human-Powered Dispute Resolution for Blockchain Smart Contracts.* [online] Available from: https://medium.com/jurisproject/introducing-the-juris-protocol-human-powered-dispute-resolution-for-blockchain-smart-contracts-bc574b50d8e1 [Accessed 05 May 2022].

After hearing the parties and considering evidence, the arbitrators within 30 days make a decision that is binding and subject to automatic execution by smart contract.

Another project based on the blockchain technology is *Mattereum*, which presents the layer of the legal, technological, and commercial infrastructure that governs on-chain rights control and transfer for tangible, intangible, and digital assets. Mattereum supports a decentralized commercial law system, the Smart Property Register, that executes through automated smart contracts that ensure property rights, as well as dispute resolution and enforcement. This register facilitates "on-chain property transfer" through a smart contract that in effect becomes a "legal contract" without the need for legislative support.[22] A distinctive feature of this project is the "Ricardian Contracts" on which the contract protocol is based.[23] Ricardian Contracts are cryptographically verified documents signed with a digital signature and available for reading both in electronic and text form. The project involves the creation of a decentralized arbitration court, meeting the requirements of the New York Convention on Recognition and Enforcement of Foreign Arbitral Awards of 1958 (hereinafter referred to as the New York Convention). Therefore, awards of such decentralized commercial arbitration court will be enforced by national courts in nearly all of the countries in the world.[24]

A separate point must be made about *OpenBazaar Dispute Resolution (notary)*. It is a distributed program that provides an on-line trading platform for any type of merchandise using cryptocurrencies.[25] It is a distributed network where the parties and transactions are anonymous.[26] A core element of the OpenBazaar dispute resolution mechanism concerns the possibility of appealing to a notary who becomes an arbitrator and determines the dispute based on the evidence presented. Notaries in the OpenBazaar system are randomly chosen to provide anonymity for keeping the system secure. An important feature of OpenBazaar's approach

[22] Allen, D., Lane, A. M. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*, 25, pp. 75–101.

[23] Zagaynova, M. (2018) *Obzor ICO proekta Mattereum.* [online] Available from: https://ffc.media/ru/overviews/ico-mattereum-project-review/ [Accessed 21 June 2022].

[24] Allen, D., Lane, A. M. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*, 25, pp. 75–101.

[25] Sanchez Dr W. *Dispute Resolution in OpenBazaar.* [online] Available from: http://docs.openbazaar.org/03.-OpenBazaar-Protocol/ [Accessed 21 June 2022].

[26] Kaal, W. A. and Calcaterra, C. (2018) Crypto Transaction Dispute Resolution. *Business Lawyer.* Available from: http://dx.doi.org/10.2139/ssrn.2992962 [Accessed 05 May 2022].

is connected with the ability of the parties to choose the notary pools as an expert in certain fields of law. Besides, OpenBazaar has an appeal system that includes randomly selecting new notaries from the pool chosen by the parties earlier.

2.2.2 CROWDSOURCED DISPUTE RESOLUTION

This group includes projects that provide for the establishment of fundamentally new, unique platforms based on blockchain technology and specifically designed to resolve disputes arising from smart contracts. Their essence is an attempt to create a quasi-judicial system, where the judges (members of the jury) are registered on the relevant platform users who are elected through the method of generating random numbers, remaining anonymous to the parties. Each of the judges votes separately; after the voting is completed, the system counts the votes and determines the outcome of the dispute. Then the decision is automatically executed using a smart contract. Another important characteristic of such projects is the use of codes of non-state regulation in the dispute resolution process.[27]

It has to be noted that crowdsourced dispute resolution is not new. For example, more than twenty years ago iCourthouse pioneered the notion of online crowdsourcing in civil cases and ten years ago eBay India's Community Court leveraged the best judgement of other eBay users to decide whether a contested eBay review should be deleted. The following examples of crowdsourced dispute resolution on the blockchain go even further with this model, however, by tokenizing the process. In other words, jurors vote with funds (generally cryptocurrency), which they lose if they are on the losing side. In contrast, jurors on the winning side generally gain some reward. This creates a market for accurate crowdsourced resolution outcomes.[28]

One example is *Oath*, a project based on the Ethereum platform. The model of OATH's dispute resolution is related to the idea of a jury trial. When entering into a smart contract, the parties can use the provided dispute resolution protocol (Smart Arbitration Plan). In the case of a dispute, the protocol is converted into a Smart Arbitration Case. After

---

[27] Zasemkova O. (2020) Methods of Resolving Disputes Arising from Smart Contracts. *Lex Russica,* 73 (4), p. 20.

[28] Rule, C. and Nagarajan, C. (2011) Crowdsourcing Dispute Resolution Over Mobile Devices. In: Poblet, M. (ed.) *Mobile Technologies for Conflict Management. Law, Governance and Technology Series, vol 2.* Dordrecht: Springer, pp. 93–100.

that, the parties set the parameters for resolving dispute: the number of jurors (any odd number in the range from 11 to 101); the percentage of votes required to make a decision (from 51 to 100 %). Juries are selected randomly from the users of the blockchain platform. The decision is made solely on the basis of common sense (Common sense), based on the study of the terms of the contract, witness statements and other evidence. The decision can be appealed within 5 days from the date of its issuance by repeating the procedure but with other jurors.[29]

Like Oath, *Kleros* promises inexpensive and transparent, online dispute resolution using crowdsourcing theory. The mechanism is similar to Oath, advocating for an opt-in court platform that uses "crowdsourced jurors". First, smart contracts have to designate Kleros as their arbitrator in cases of dispute, including the type of court (Kleros is developing an ecosystem of specialized courts) and the number of juries to be involved (idem). When a dispute arises, Kleros randomly assigns the dispute to a jury of crowdsourced, self-selected experts, who analyze the evidence and vote for a verdict. Jurors are penalized for communicating with each other, and must "justify" their votes so that the parties can later understand their decisions. A smart contract then transfers the money to the winning party. Oracles are engaged to provide real-world data to assist dispute resolution.[30]

A similar platform is *Jur.io* that advertises itself as a free service to users for creating and securing smart contracts and resolving contract disputes within 24 hours. Accordingly, Jur's key promise seems to be speed and security in smart contracting.[31] Its unique feature is the opportunity to create their own hub (a "specialized oracle") which operates on special rules for users in particular industries.[32] Additionally, the Jur platform provides tools for signing contracts, and creating and reselling contract templates.[33]

---

[29] *OATH Protocol. Blockchain Alternative Dispute Resolution Protocol. Version 2.6.0.* Available from: https://oaths.io/files/OATH-Whitepaper-EN.pdf [Accessed 15 June 2022].

[30] Allen, D., Lane, A. M. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*, 25, pp. 75–101.

[31] *JUR.Io – platforma kotoray pomozet razreshit finansovye spory mezdy investorami i srartupami.* (2018) [online] Available from: https://invest4all.ru/obzory-i-otchyoty/obzory-kraudsejlov-ico/jur-io-platforma-kotoraya-pomozhet-razreshit-finansovye-spory-mezhdu-investorami-i-startapami [Accessed 15 June 2022].

[32] Ibid.

[33] Ibid.

It is worth pointing out that the above-mentioned platforms have a dispute resolution mechanism with the following characteristics: (i) adjudicator expertise in dispute resolution and law; (ii) independence (neutral and anonymous adjudicators); (iii) impartiality (random selection of judges without vested interests); and (iv) transparency (all procedures are documented and rationalized).[34]

3. SHORTCOMINGS OF THE TRADITIONAL ARBITRATION INSTITUTIONS AND BLOCKCHAIN ARBITRATION

There are several drawbacks associated with "off-chain" arbitration. Firstly, courts could only force the parties to execute a secondary transaction or otherwise pay remedies for a smart contract that created damages for one of the parties. Courts are not able to change the terms of the given smart contract that was executed according to its parameters and added to the blockchain because they could not change the existing code. Because of these inherent limitations, courts are not able to render resolutions to disputes arising from blockchain-based smart contracts. Secondly, it is worth mentioning that high price is another disadvantage of traditional arbitration institutions. In particular, Tang Z. S. states that the average online consumer contract value is USD60, whereas an exemplary UK provider of ODR services charges between GBP25 and GBP850 for a resolution of consumer disputes. Therefore, even the lowest charge of GBP25 will be disproportionately expensive compared with the average value of the consumer disputes.[35]

Moreover, traditional arbitration institutions are characterized by a slow speed of dispute resolution. However, in the online environment, people would often like to get a quick decision. In relation to the incapability of traditional dispute resolution to resolve numerous online disputes, it should be pointed out that when the number of disputes runs into the millions, human-powered dispute resolution cannot handle the scale of disputes.[36]

---

[34] Allen, D., Lane, A. M. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review*, 25, pp. 75–101.

[35] Tang, Z. S. (2015) *Electronic consumer contracts in the conflict of laws.* 2nd ed. Oxford: Hart Publishing, p. 373.

[36] Dimov, D. (2017) *Crowdsourced Online Dispute Resolution.* [online] Ph.D. Leiden University.

Therefore, traditional arbitration mechanisms could not be the only possible recourse for smart contract disputes.[37]

The first drawback of "on chain" arbitration concerns the enforceability of awards. In other words, arbitral awards rendered through online arbitration may not be recognized and enforced under the New York Convention because, pursuant to Article 2 of the New York Convention, it applies only to agreements "in writing".[38] However, online arbitral agreements would appear to satisfy the writing requirements of the convention. The reason is that, under most national legislation, electronic writings are considered equivalent to traditional writings.[39] As a corollary, it is uncertain whether an award issued pursuant to an arbitration agreement contained in the code of a smart contract would be capable of being enforced.

The second drawback is the lack of trust in the procedures caused by non-face-to-face communication. People who do not trust each other may act tentatively and keep important information to themselves. As a result, disputants participating in ODR processes may not disclose all the relevant information to online arbitrators.[40] Moreover, criminals may exploit the information security vulnerabilities of the ODR platform in order to obtain unauthorized access to information related to the dispute and the disputants. That is why the ODR provider should use information security practices.[41]

The third drawback concerns the parties who may not be familiar and comfortable with the relevant technology. Besides, it should be noted that the legal qualification of arbitrators may be crucial for parties who want to choose arbitrators with the special technical knowledge to adjudicate certain disputes.

---

[37] Kaal, W. A. and Calcaterra, C. (2018) Crypto Transaction Dispute Resolution. *Business Lawyer*. Available from: http://dx.doi.org/10.2139/ssrn.2992962 [Accessed 05 May 2022].

[38] *Convention on the Recognition and Enforcement of Foreign Arbitral Awards,* 10 June 1958. Available from: http://www.newyorkconvention.org/11165/web/files/original/1/5/15432.pdf [Accessed 23 June 2022].

[39] Cortes, P. (2010) *Online Dispute Resolution for Consumers in the European Union. Routledge Research in IT and E-commerce Law.* London: Routledge, Taylor & Francis Group. Available from: https://www.econstor.eu/bitstream/10419/181972/1/391038.pdf [Accessed 23 June 2022].

[40] Ibid.

[41] Lodder, A. R. and Zeleznikow, J. (2005) Developing an Online Dispute Resolution Environment: Dialogue Tools and Negotiation Support Systems in a Three-Step Model. *Harvard Negotiation Law Review,* 10, pp. 287–337.

In addition, the described method of dispute resolution is obviously devoid of a standard of efficiency, since there is no possibility to limit in advance the range of checks used by arbitrators, who may not respect the accumulated experience in resolving similar cases. As a result, a decentralized court decision will become more and more resource--intensive over time, as the parties will try to determine all possible circumstances in the program code. In other words, the parties will have to discuss each dispute from the very beginning, without any knowledge of the previous cases.

Besides, problems arise with the method of selection of the arbitrators as well as ways of making their decisions. Arbitrators are selected randomly, but from a certain group of specialists in the blockchain area, which is not very big now. For that reason, there is a risk that the arbitrators will not be independent of the parties.

To sum up, neither of these two alternative mechanisms can provide an adequate environment for resolving disputes arising from smart contracts. Therefore, in the next paragraph, I introduce the design and implementation of a hybrid for the digital dispute.

4. HYBRID APPROACH

In light of the shortcomings of the available dispute resolution mechanisms for the crypto economy, it is possible to talk about instituting a hybrid approach. It means the creation of an independent, decentralized platform that integrates both approaches to the smart contract dispute resolution problem. This framework recognizes internal mechanisms of the smart contract system that will regulate disputes depending on the precise nature of the case and certain circumstances.

Parties should incorporate a mandatory dispute settlement clause directly in the smart contract code.

Such a clause may include the following provisions:

a) automatic adoption of interim measures (for example, suspension of performance of obligations under a smart contract, blocking of funds);

b) rules and deadlines for the creation of arbitration;

c) procedure and deadlines for dispute resolution;

d) procedure for the execution of arbitration awards; it means technical standards that allow smart contracts to be reversed;

e) an agreement between the parties to resolve disputes using on-chain resolution platforms. The lack of agreement between the parties should lead to resolve the dispute with an on-chain system;

f) a clause regulating dispute resolution. For instance, by including an ICC Arbitration Clause in a contract, the parties agree that their dispute will be resolved by arbitration and that the arbitration proceedings will be governed by the procedural rules in the ICC Rules of Arbitration, given the finality and binding effect of an arbitral award for the parties.

Even if the dispute was resolved with "on chain" mechanisms, the interested party should still have the right to appeal to the off-chain arbitration. In these cases, decisions reached by way of blockchain arbitration should not rise to the level of "off chain" arbitration.

To be specific, the off-chain arbitration should be viable for the following cases:

- the disputes where one party is a consumer (taking into account the level of consumer protection existing in the EU and its Member-States);
- the complex disputes (i.e. it is necessary to examine additional evidence, to assign an expert examination or to hear witness testimony);
- the procedure may lead to the disclosure of commercial secrets;
- the disputes where fundamental rights are at stake.

This last condition is due to the impossibility to predict at the moment of drafting the contract, what kind of disputes may arise between the parties in the interpretation and performance of the contract. Therefore, it should be possible for the parties to consider the dispute using traditional arbitration.

Generally speaking, on-chain resolution platforms could be used for resolving minor disputes (with a small cost), for instance cross-border consumer disputes. Moreover, they could be used for technical disputes, such as gas or share price determination and construction schedule disputes. In other words, an "on chain" arbitration system could act as an expert to resolve factual issues, such as whether a contract performance complied with technical specifications, to calculate the market value of shares or commodities, or to calculate damages. In these cases, the parties may agree that the "on chain" arbitration award will be binding.

The ability of the parties to resolve disputes with online forms is of high importance due to several benefits. Firstly, the high speed of online procedures. Off-chain arbitration is not able to cope with the huge number

of online disputes. Secondly, the absence of on-chain resolution would negate key blockchain benefits and would undermine the evolution of the crypto economy.

However, on-chain arbitration requires the adaptation to the existing legal regulation, primarily to the requirement of the New York Convention to an arbitration agreement to be in writing. Otherwise, smart contracts run the risk of not being enforced under the New York Convention, unless they have an equivalent traditional word-format contract signed by both parties. In this regard, it seems appropriate to have a hybrid version of smart contracts, whereby there is a text-based version of the same force in addition to the encrypted-coded-language smart contract.

All these considerations are compelling and favor a hybrid approach. Given the current legal framework, fully "on chain" arbitration will not become a reality in the nearest future. At the same time, prospects of a hybrid approach are much more likely. It will reflect the complex nature of blockchain technologies and the diversity of smart contracts used in a dynamically competitive environment. On the one hand, the possibility of using "on chain" arbitration will lead to speedy, less-costly awards, to the benefit of parties in various specific sectors. Thus, the essence of a smart contract will be reflected in comparison with a traditional contract. On the other hand, "off chain" arbitration in certain cases seems to be unavoidable given the legal realities of the modern world.

5. CONCLUSION

All in all, building and implementation of the effective dispute resolution into smart contracts will be a crucial step in achieving level of certainty in crypto transactions and facilitating the broadening evolution of the crypto economy. Different mechanisms described above for resolving smart contracts demonstrate various possibilities, opting human-driven resolution systems or crowdsourced systems.

The development and introduction of new technologies should be convenient for the participants, diminishing their risks and making it possible to protect their rights in a faster manner. Besides, the use of technology could be advantageous for the justice system, which could be relieved of the burden of deciding certain kinds of disputes.

The hybrid approach that I suggest in this article addresses problems that neither the "on chain" nor "off chain" approaches can address

separately. I argue that for some reasons, hybrid solutions are more adequate given the framework of the Internet Age. The world is rapidly changing, and laws will have to adapt to this rising tide. As such, the growth of smart contracts will require adaptation by the legal profession and modification of approaches to dispute resolution. In doing so, though, contract law should operate according to its traditional canons and categories, through a modification and supplementation of existing rules and procedures.[42] And these technologies should be seen as an improvement of existing contractual structures in terms of their effectiveness. They cannot definitely change the essence of dispute resolution relationships between the parties.

Without a doubt, using a hybrid architecture can substantially improve the dispute resolution from smart contracts while retaining existing traditional law rules and principles. However, there is a room for specification of the individual conditions of "on chain" and "off chain" arbitration.

LIST OF REFERENCES

[1] Allen, D., Lane, A. M. and Poblet, M. (2019) The Governance of Blockchain Dispute Resolution. *Harvard Negotiation Law Review,* 25, pp. 75–101.

[2] *Arbitraznyu zentr pri RSPP.* [online] Available from: https://arbitration-rspp.ru/about/structure/boards/digital-disputes/ [Accessed 04 May 2022].

[3] Chamber of Digital Commerce. (2018) *Smart Contracts: Is the Law Ready?* Available from: https://www.theblockchaintest.com/uploads/resources/CDC%20-%20Smart%20Contract-Is%20the%20Law%20Ready%20-%202018%20-%20Sep.pdf [Accessed 02 May 2022].

[4] Clément, M. (2019) Smart Contracts and the Courts. In: DiMatteo, L., Cannarsa, M. and Poncibò, C. (eds.) The *Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms.* Cambridge University Press, pp. 271–287.

[5] *Convention on the Recognition and Enforcement of Foreign Arbitral Awards,* 10 June 1958. Available from: http://www.newyorkconvention.org/11165/web/files/original/1/5/15432.pdf [Accessed 23 June 2022].

[42] Pardolesi, R. and Davola, A. (2019) What Is Wrong in the Debate About Smart Contracts. *SSRN Electronic Journal.* Available from: https://www.researchgate.net/publication/331834837_What_Is_Wrong_in_the_Debate_About_Smart_Contracts [Accessed 23 June 2022].

[6] Cortes, P. (2010) *Online Dispute Resolution for Consumers in the European Union. Routledge Research in IT and E-commerce Law.* London: Routledge, Taylor & Francis Group. Available from: https://www.econstor.eu/bitstream/10419/181972/1/391038.pdf [Accessed 23 June 2022].

[7] *The Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce.* [online] Available from: https:// blockchaincourt.org/ [Accessed 02 May 2022].

[8] The Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce (2019). *The Rules of the Court of Arbitration of the Polish Blockchain and New Technology Chamber of Commerce.* Available from: https://blockchaincourt.org/wp-content/uploads/2019/07/The-Rules-of-the-Court-of-Arbitration-ENG.pdf [Accessed 04 May 2022].

[9] Dimov, D. (2017) *Crowdsourced Online Dispute Resolution.* [online] Ph.D. Leiden University.

[10] De Filippi, P. and Wright A. (2018) *Blockchain and the Law: The Rule of Code.* Cambridge, Cambridge, MA: Harvard University Press, 300.

[11] Grimmelmann, J. (2019) All Smart Contracts are Ambiguous. *Journal of Law & Innovation,* 2 (1). Available from: https://www.law.upenn.edu/live/files/9782-grimmelmann-all-smart-contracts-are-ambiguous [Accessed 02 May 2022].

[12] International Chamber of Commerce (2018). *ICC Dispute Resolution Bulletin. Issue 1.* Available from: https://www.hoganlovells.com/~/media/hogan-lovells/pdf/2018/2018_12_13_icc_robots_arbitrator.pdf [Accessed 02 May 2022].

[13] *JUR.Io – platforma kotoray pomozet razreshit finansovye spory mezdy investorami i srartupami.* (2018) [online] Available from: https://invest4all.ru/obzory-i-otchyoty/obzory-kraudsejlov-ico/jur-io-platforma-kotoraya-pomozhet-razreshit-finansovye-spory-mezhdu-investorami-i-startapami [Accessed 15 June 2022].

[14] Kaal, W. A. and Calcaterra, C. (2018) Crypto Transaction Dispute Resolution. *Business Lawyer.* Available from: http://dx.doi.org/10.2139/ssrn.2992962 [Accessed 05 May 2022].

[15] Kerpelman, A. J. (2018) *Introducing the Juris Protocol: Human-Powered Dispute Resolution for Blockchain Smart Contracts.* [online] Available from: https://medium.com/jurisproject/introducing-the-juris-protocol-human-powered-dispute-resolution-for-blockchain-smart-contracts-bc574b50d8e1 [Accessed 05 May 2022].

[16] Lodder, A. R. and Zeleznikow, J. (2005) Developing an Online Dispute Resolution Environment: Dialogue Tools and Negotiation Support Systems in a Three-Step Model. *Harvard Negotiation Law Review,* 10, pp. 287–337.

[17] *OATH Protocol. Blockchain Alternative Dispute Resolution Protocol. Version 2.6.0.* Available from: https://oaths.io/files/OATH-Whitepaper-EN.pdf [Accessed 15 June 2022].

[18] Pardolesi, R. and Davola, A. (2019) What Is Wrong in the Debate About Smart Contracts. *SSRN Electronic Journal.* Available from: https://www.researchgate.net/publication/331834837_What_Is_Wrong_in_the_Debate_About_Smart_Contracts [Accessed 23 June 2022].

[19] Rodrigues, U. (2018) Law and the Blockchain. *Iowa Law Review,* 104. Available from: https://ilr.law.uiowa.edu/print/volume-104-issue-2/law-and-the-blockchain/ [Accessed 02 May 2022].

[20] Rule, C. and Nagarajan, C. (2011) Crowdsourcing Dispute Resolution Over Mobile Devices. In: Poblet, M. (ed.) *Mobile Technologies for Conflict Management. Law, Governance and Technology Series, vol 2.* Dordrecht: Springer, pp. 93–100.

[21] Sanchez Dr W. *Dispute Resolution in OpenBazaar.* [online] Available from: http://docs.openbazaar.org/03.-OpenBazaar-Protocol/ [Accessed 21 June 2022].

[22] Schmitz, A. J. and Rule, C. (2019) Online Dispute Resolution for Smart Contracts. *Journal of Dispute Resolution. University of Missouri School of Law Legal Studies Research Paper,* 2019 (11). Available from: https://ssrn.com/abstract=3410450 [Accessed 12 April 2022].

[23] Schmitz, A. and Rule, C. (2019) Online Dispute Resolution for Smart Contracts. *Journal of Dispute Resolution,* 2, pp. 103–125.

[24] Sillanpaa, T. (2020) Freedom to (Smart) Contract: The Myth of Code and Blockchain Governance Law. *IALS Student Law Review,* 7 (2). Available from: https://journals.sas.ac.uk/lawreview/issue/view/582 [Accessed 02 May 2022].

[25] Szczudlik, K. (2019) *"On-chain" and "off-chain" arbitration: Using smart contracts to amicably resolve disputes.* [online] Available from: https://newtech.law/en/on-chain-and-off-chain-arbitration-using-smart-contracts-to-amicably-resolve disputes [Accessed 02 May 2022].

[26] Tang, Z. S. (2015) *Electronic consumer contracts in the conflict of laws.* 2nd ed. Oxford: Hart Publishing, p. 373.

[27] Zagaynova, M. (2018) *Obzor ICO proekta Mattereum.* [online] Available from: https://ffc.media/ru/overviews/ico-mattereum-project-review/ [Accessed 21 June 2022].

[28] Zasemkova O. (2020) Methods of Resolving Disputes Arising from Smart Contracts. *Lex Russica,* 73 (4), p. 20.

[29] Zaslowsky, D. (2018) *What to Expect When Litigating Smart Contract Disputes.* [online] Available from: https://www.law360.com/articles/1028009/what-to-expect-when-litigating-smart-contract-disputes [Accessed 02 May 2022].

DOI 10.5817/MUJLT2022-2-3

DATA PROTECTION HAS ENTERED THE CHAT: ANALYSIS OF GDPR FINES[1]

by

NIMRÓD MIKE[*]

Before the adoption of the EU-GDPR, researchers remarkably argued on law enforcement of personal data protection being „toothless" and a "paper tiger". Almost three years after its enforcement date, the GDPR fines are increasing, and the world is beginning to witness the effect of sizeable fines awarded to organizations. This analysis aims to discover potential correlations between GDPR fines, and equally the lack of them. Such correlations might help to tap into trends that are followed by Data Protection Authorities (DPA) in their fining practices. This paper specifically describes the fines issued by the Romanian DPA, while also containing qualitative research findings extracted from discussions with interview subjects. The aim of this paper is to evaluate the possibility to construct a prediction model that is based on linear regression analysis and provide for future direction on the field of legal data analysis.

KEY WORDS

GDPR fines, data analytics, R-programming, fine calculation

1. INTRODUCTION

Data protection law has a long history in Europe, but it appears to have come to the attention of the individual from 25th of May 2018, when the EU-GDPR[2] (GDPR) replaced its predecessor, the Directive 95/46/EC[3] (DPD). Although the DPD laid down much of the legal groundwork for EU-wide data protection, its national adaptations, legal interpretations, and

[1] The present publication is the outcome of the project „From Talent to Young Researcher project aimed at activities supporting the research career model in higher education", identifier EFOP-3.6.3-VEKOP-16-2017-00007 co-supported by the European Union, Hungary and the European Social Fund.

[*] E-mail: nimrod.mike@uni-corvinus.hu, Assistant lecturer, Corvinus University of Budapest, Institute of Information Technology, Hungary.

enforcement varied across both the member states and different EU institutions[4]. With massive differences resulting between member states[5], the academia simply called it a "paper tiger"[6]. Hence the law of the land for Europe became a regulation.

According to Blutman, a regulation has general application, is binding in his entirety and directly applicable in all European Union countries[7]. A regulation is then a stronger means to provide legislative harmonization across member states of EU. The shift from directive to regulation was necessary due to the rapidly changing environment surrounding the processing of personal data. Technological advance and massive industrial research and development are translating into newer means of processing. Many concerns were raised towards the excessive processing of personal data with the introduction of the new technologies, such as Web 2.0 services[8], Cloud-computing[9], Smart cards[10] and others. These methods heavily rely on customer's personal contribution since the core

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union* (L 119, 4.5.2016, p. 1–88). Available from: https://eur-lex.europa.eu/eli/reg/2016/679 [Accessed 4 February 2021].

[3] Directive (EC) 95/46 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 *Official Journal of the European Union* (L281, 23/11/1995 P. 0031 – 0050). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex %3A31995L0046 [Accessed 4 February 2021].

[4] Ruohonen J. and Hjerppe K. (2020) The {GDPR} enforcement fines at glance, Information Systems 106, p.1. Available from http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf [Accessed 5 February 2021].

[5] Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from https://www.jipitec.eu/issues/jipitec-8-1-2017/4533 [Accessed 10 February 2021].

[6] Ruohonen J. and Hjerppe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, p.1. Available from http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf [Accessed 5 February 2021].

[7] Blutman, L. (2014), Az Európai Unió joga a gyakorlatban, Budapest, HVG-ORAC, p.158.

[8] Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over time Web 2.0 has been used more as a marketing term than a computer-science-based term. Blogs, wikis, and Web services are all seen as components of Web 2.0.

[9] Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to manage applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "*the Internet*," so the phrase *cloud computing* means "a type of Internet-based computing," where different services — such as servers, storage, and applications — are delivered to an organization's computers and devices through the Internet.

of the software is based on the mutual trust between the service provider and the user. As consumers were increasingly concerned about breaches of privacy, loss of trust was translated into lost opportunities and revenue for companies. Recent high profile data breaches have pushed consumers change service providers who did not adequately protect personal data. The high-profile data breaches are also the motivation behind growing monetary penalties[11]. However, it is necessary to separate infringement cases based on the quoted articles by the DPAs as not all penalties are results of personal data breaches[12].

GDPR fines are increasing, and the world is witnessing the effect of sizeable fines awarded to organizations. Golla argues that Data Protection Authorities (DPAs) should grow teeth by issuing more significant monetary sanctions[13]. He also emphasized that there were big differences in the maximum amounts of administrative fines between the different member states in the pre-GDPR era[14]. While Romanian Law (maximum circa €11,000) and Slovenian Law (€12,510) allowed for relatively low fines, Spanish (€600,000) and UK Laws (£500,000) had much higher thresholds[15]. Indeed law enforcement of personal data protection was deemed to be „toothless"[16].

This analysis aims to discover potential correlations between GDPR fines and the lack of them. The correlations might help to tap into trends that are followed by DPAs in their fining practice. This paper specifically describes the fines issued by the Romanian DPA. The main question imposed herein

---

[10] A small electronic device about the size of a credit card that contains electronic memory and an embedded integrated circuit (IC). Smart cards containing an IC are sometimes called *Integrated Circuit Cards (ICCs).* Smart cards are used for a variety of purposes, including storing a patient's medical records; storing digital cash; generating network IDs (similar to a token).

[11] At the moment of writing the highest amount has been given to Alphabet Inc. by the French DPA. Available at: https://www.enforcementtracker.com/ETid-23 [Accessed 13 February 2021]

[12] Aricle 4. para (12) of GDPR provides that 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[13] Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law 8* (1). Available from https://www.jipitec.eu/issues/jipitec-8-1-2017/4533 [Accessed 10 February 2021].

[14] Ibid.

[15] Ibid.

[16] Albrecht, J. P. (2016), Privacy enforcement in search of its base, In: David Wright and Paul De Hert (eds) *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer International Publishing, p. 47.

is that with the adoption of GDPR can we expect bigger fines or more frequent ones for data protection violations?

In this study both quantitative and qualitative research methods are used to answer the research question framed above. To evaluate the trends in fine setting, the workings of various DPAs are studied. Fine calculation models that have been published by the DPAs are an important part of this discovery process. Further, custom models framed by practitioners are also relatable, thus included in the analysis. The novel approach in qualitative research is the application of supervised machine-learning on a constructed dataset[17]. Through supervised machine learning the algorithms may discover variables[18] that play a significant role in determining the administrative fine. Using the dataset, we construct three different types of trained regression algorithms (models) in R programming language. The models deployed in the analysis are based on techniques of regression tree[19], random forest[20] and linear regression[21].

This examination will potentially provide more transparency and offer insights on the profile of companies that are more exposed to such legal risks as receiving a fine for violating GDPR provisions. To the same extent, it may offer conclusions underlining total randomization and selective arbitration in this respect. Nonetheless, the research ideally will explain how existing guidelines on fine setting can impact the practice of DPAs.

The structure of the paper is as follows: the introduction in Section 1 serves the reader with general and wide overview about the topic itself. The introduction is followed by Section 2, where the aim is the presentation

---

[17] The primary source for data collection is the GDPR Enforcement Tracker maintained by CMS law (www.enforcmenttracker.com). The selection criteria for constructing the dataset is described in detail at Section 4.1.

[18] As a key action within the dataset preparation, we develop additional attributes expressed as variables. These variables are tied to the business metrics of the companies that received an administrative fine for GDPR infringements. The variable glossary is presented in Section 4.1 and Section 4.5.1 accordingly.

[19] UC Business Analytics R Programming Guide (2018) *Regression Trees*. [online]. Available from: http://uc-r.github.io/regression_trees [Accessed 5 March 2021]. Basic regression trees partition a data set into smaller groups and then fit a simple model (constant) for each subgroup.

[20] UC Business Analytics R Programming Guide (2018) *Random Forests*. [online]. Available from: http://uc-r.github.io/random_forests [Accessed 5 March 2021]. Random forests are responsible for building a large collection of de-correlated regression trees. Usually these have a good predictive performance.

[21] UC Business Analytics R Programming Guide (2018) *Linear Regression.* [online]. Available from: http://uc-r.github.io/linear_regression [Accessed 5 March 2021]. Linear regression is a useful tool for predicting a quantitative response and it is a widely used statistical learning method.

of principles established by the European Data Protection Board (EDPB) in their Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679[22]. Section 3 provides on existing calculation models proposed by DPAs. Section 4 presents a possible new approach to predict GDPR fines supported by data analytics applying a linear regression model constructed in R programming language. Section 4 also elaborates on the case study of the administrative fines issued by the Romanian DPA. The model is presented to understand how fines are applied. Section 5 finally delivers the conclusion, limitations, and future work.

2. PRINCIPLES OF SETTINGS FINES

From a thorough reading of the EDPB Guidelines[23] four main principles can be extracted to the application of administrative fines. Table 1 summarizes the principles.

	Name	Summary
P1	Equivalent sanctions	Infringement of the Regulation should lead to the imposition of equivalent sanctions.
P2	Effective, proportionate, and dissuasive fines	As with all corrective measures chosen by the DPAs, administrative fines should be effective, proportionate, and dissuasive.
P3	Case-by-case assessment	The competent supervisory authority will make an assessment in each individual case.
P4	Active participation of DPAs	A harmonized approach to administrative fines in the field of data protection requires active participation and information exchange among DPAs.

Table 1. Principles of fines applied by DPAs

One might consider that the role of DPAs are only to issue fines, although, the powers vested in DPAs are far more reaching than the implementation of fines. The tasks of DPAs as per Art. 58 of GDPR provide a wide array

[22] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], pp. 1-17.

[23] *Op. cit*., p.5.

of esponsibilities. Figure 1 presents the typology of powers sitting with the DPAs.

Figure 1. Powers of DPAs based on Art 58 GDPR.

Further, the EDPB Guidelines provide that the DPAs must identify the most appropriate corrective measures to address GDPR infringements. Figure 2 presents the corrective measures categories currently recognized.

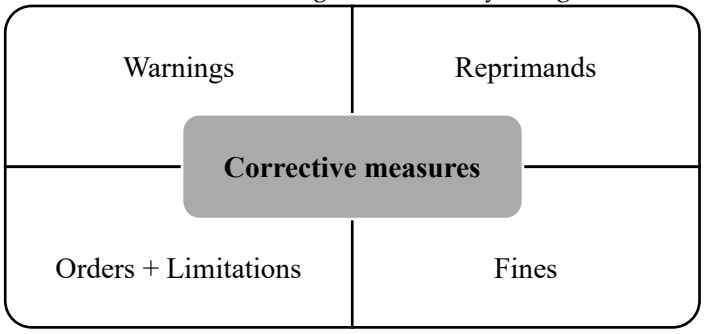

Figure 2. Categories of corrective measures

Based on Art. 58 (2) a) warnings are typically issued to a controller or processor if the intended processing operations are likely to infringe provisions of GDPR. The DPAs shall issue reprimands to a controller

or a processor where processing operations have infringed provisions of GDPR, but the infringement consists of "minor infringements".[24]

Orders as corrective measures can be of multiple types:

- The DPA may order the controller or processor to comply with data subject requests (DSRs) [art. 58 (2) c)];
- to bring processing operations into compliance with GDPR provisions in a specified manner and within a specified period [art. 58 (2) d)];
- to communicate a personal data breach to the data subject(s) [art. 58 (2) e)];
- to limit temporarily or permanently the processing [art. 58 (2) f)];
- to rectify, delete or restrict the processing of personal data and to notify recipients of such personal data pursuant to Art. 17 (2) and Art. 19 [art. 58 (2) g)];
- to withdraw a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43 [art. 58 (2) h)];
- and finally, to order the suspension of data flows to recipient in a third country or to an international organization [art. 58 (2) j)].

In addition, the DPAs can provide administrative fines, depending on the circumstances of each individual case [art. 58 (2) i)].

2.1 EQUIVALENT SANCTIONS

Recital (10) of GDPR calls for equivalent level of protection of personal data in Member States. The motivation behind enshrining that sanctions are equivalent are also further debated in Recitals (11) and (13). This provision is backed up by S. Golla[25]. Throughout this equivalency EDPB also stresses that the GDPR calls for a greater consistency than the DPD when imposing sanctions[26]. The principle to be followed is to prevent different corrective

[24] Recital 148 introduces the notion of "minor infringements". Such infringements may constitute breaches of one or several of the Regulation's provisions listed in article 83 (4) or (5). The assessment of the criteria in article 83 (2) may however lead the supervisory authority to believe that in the concrete circumstances of the case, the breach for example, does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation in question. In such cases, the fine may (but not always) be replaced by a reprimand. *Op. cit.*, p. 9.

[25] Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from https://www.jipitec.eu/issues/jipitec-8-1-2017/4533 [Accessed 10 February 2021].

measures being chosen by the DPAs in similar cases[27]. C. Barrett further argues that P1 encourages DPAs to apply a consistent approach in their "use of corrective powers," including the application of administrative fines in particular[28].

Practitioners denote that the principle of equivalence can also be found in the case law of the European Court of Justice (CJEU), even though its meaning is not exactly the same as that determined by the EDPB[29]. Indeed, as the CJEU case law indicates this should mean the sanctions to violations of national law are the same as to sanctions applied by EU law[30]. It is really important to highlight what Maxwell and Gateu are accurately pointing out on this principle: it demands the non-discrimination in the application of sanctions[31]. Non-discrimination is of utmost importance to ensure legal certainty. Regarding the scope of this paper, such obligation of non-discrimination also serves to determine why GDPR fines may be predictable.

No one would go on record saying that privacy cannot be monetized. To the same extent there is a good chance no one would dare to say that GDPR infringements cannot be translated into economic values. The mere fact that it is difficult does not mean it is impossible. S. Greengard says that it is certain, amid a litany of security breaches and breakdowns, from Equifax (2017) to Cambridge Analytica (2018), there is a growing focus on data privacy[32]. Frischmann in the same article further denotes that GDPR, more than anything else, represents the ongoing battle between unfettered

---

[26] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 5.

[27] Ibid.

[28] Barrett, C. (2020) Emerging Trends from the First Year of EU GDPR Enforcement, *ABA – American Bar Association Data, Spring 2020* 16 (3). Available from https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/emerging-trends-the-first-year-eu-gdpr-enforcement/#25 [Accessed 25 January 2021].

[29] Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr [Accessed 20 January 2021], p. 103.

[30] *Op. cit*, p. 104.

[31] *Op. cit*, p. 105.

[32] Greengard, S. (2018) Weighing the impact of GDPR, *Communications of the ACM 61* (11), p. 17.

capitalism and human dignity and that the whole point of it is that it is not designed to be an efficient regulation for businesses[33].

2.2 EFFECTIVE, PROPORTIONATE, AND DISSUASIVE FINES

To best assess if a fine may fulfil the requirements of P2, a case-by-case examination is crucial. The EDPG Guidelines hint towards three possible objectives pursued by the corrective measures chosen, that is:

- re-establishing the compliance with rules,
- punish unlawful behaviour,
- or a combination of the two[34].

According to Maxwell – Gateu[35]:

> *"Effectiveness" means that national law should not render the enforcement of EU law virtually impossible[36]. Effectiveness also includes the principle of equivalence and non-discrimination as regards comparable violations of national law[37].*
>
> *"Proportionality" means that sanctions should not exceed what is appropriate and necessary to attain the objective legitimately sought by the legislation, and that when there is a choice between several appropriate measures, recourse must be had to the least onerous, and the disadvantages caused must not be disproportionate to the aims pursued[38].*
>
> *"Dissuasiveness" means that the application of the penalty must result in the party having violated the law being substantially worse off than would be the case if he complied with the law. This requires, at a minimum, that*

---

33 *Op cit*, p. 18.

34 Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 01 February 2021], p.6.

35 Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr [Accessed 20 January 2021], pp. 103-104.

36 Judgement of Comet BV v Produktschap voor Siergewassen, Case C-45/76, ECLI:EU:C:1976:191, paragraph 16.

37 Ibid.

38 Judgement of Ute Reindle v. Bezirkshauptmannschaft Innsbruck, C- 443/13, ECLI:EU:C:2014:2370, paragraph 39.

the penalty be sufficiently high so that the guilty party loses any benefit that arose because of its illegal behaviour[39]*."*

According to EDPB, a more precise determination of P2, will result from the emerging practices of DPAs and CJEU case-law overtime[40]. The reason behind not citing the CJEU case –law, might be that the EDPB does not wish to limit the potential of DPAs forming new trends in applications of fines. The potential to apply incentives to controllers and processors is given to the DPAs. The GDPR calls for a wide range of corrective measures, the thresholds of administrative fines being raised significantly.

The EDPB Guidelines are also putting an end to a discussion on the subject matter of what should be considered an 'undertaking' in the light of GDPR. Concerns were raised towards that several language versions of use an identical term for what is described as an "undertaking" in Article 83 GDPR and as an "enterprise" Article 4 (18) GDPR (English version)[41]. Recital (150) refers to Art. 101 and 102 TFEU[42]. The undertaking means an economic unit, which may be formed by the parent company and all involved subsidiaries (i.e. an entire corporate group will be considered an undertaking). The CJEU case law definition also confirms that the concept of an undertaking encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed"[43]. In another case the definition says that an undertaking must be understood as designating an economic unit even if in law that economic unit consists of several persons, natural or legal[44].

---

[39] Judgement of LCL Le Crédit Lyonnais v. Fesih Kalhan, Case C- 565/12, ECLI:EU:C:2014:190, paragraph 51.

[40] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 6.

[41] Golla, S. (2017) Is Data Protection Law Growing Teeth? Current Lack of Sanctions in Data Protection Law and Administrative Fines under GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from https://www.jipitec.eu/issues/jipitec-8-1-2017/4533 [Accessed 10 February 2021].

[42] Consolidated versions of Treaty on European Union and Treaty on Functioning of European Union - Consolidated version of Treaty on Functioning of European Union - Protocols - Annexes - Declarations annexed to Final Act of Intergovernmental Conference which adopted Treaty of Lisbon, signed on 13 December 2007 - Tables of equivalences. *Official Journal of European Union* (C 326, 26/10/2012 P. 0001 – 0390). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12016ME%2FTXT [Accessed 22 January 2021].

[43] Judgement of Höfner and Elsner v Macrotron GmbH, Case C-41/90, ECLI:EU:C:1991:161, paragraph 21.

[44] Judgement of Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos SA, Case C-217/05, ECLI:EU:C:2006:784, paragraph 40.

2.3 CASE-BY-CASE ASSESSMENT

P3 is a direct consequence of the requirements set out in P2. For the corrective measures to take effect, be proportionate and dissuasive, these have to be customized based on the particularities of the case. Tailoring can be done based on aggravating and mitigation factors. The baseline is Art. 83 (2) of GDPR for such assessments. Indeed, fines are important tool that DPAs should use in appropriate circumstances, and these should not be qualified as last resort, nor to shy away from their use[45]. Yet, if the fines are used too often or being excessive in their nature, it would seriously undermine their legitimacy. The DPAs are not meant to be bloodthirsty. Their powers are advisory, not only corrective. Thus, the DPAs are put to a test of conflict management.

2.4 ACTIVE PARTICIPATION OF DPAS

This last principle is just the endorsement of the consistency mechanism desired by the GDPR. With the progressive tendencies of GDPR fines, DPAs should have active information exchange hard coded in their activities. To effectively learn from each other, DPAs should participate to regular workshops[46].

Acknowledging that some national DPAs are younger than others, they might lack experience in organization and procedures. The cure to this and the application of consistency is that DPAs in a more mature state are stepping in to function as a role-model. The question arises, whether this would threaten the independency of each DPA. The answer is most probably not – DPAs should be conscious about their legal status and identify themselves as independent authorities, however teamwork should characterize their work.

The EU reform on personal data protection provides a strong template. This template needs to be applied consistently across the EU. Consequently, personal data should be exchanged freely between member states of EU. If there is one standard of protection, internal boundaries will not find their place anymore. Same applies to enforcement of GDPR infringements. The DPAs have now the mission to coordinate their activities

---

[45] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 7.

[46] *Op. cit*, p. 8.

at a previously untested level. There might be a strong opposition in the corporate arena[47], but the DPAs should stand their ground firmly. The EDPB is also entrusted with issuing binding decisions based on Art. 65 of GDPR on disputes arising between DPAs relating to the determination of the existence of an infringement[48]. The first decision to be issued concerned a draft decision of the Irish DPA on Twitter International Company.

2.5 CRITERIA FRAMEWORK FOR P1-P4

The way DPA administer fines is based on the objective evaluation of the facts. The evaluation procedure consists of three basic steps presented in Figure 3.

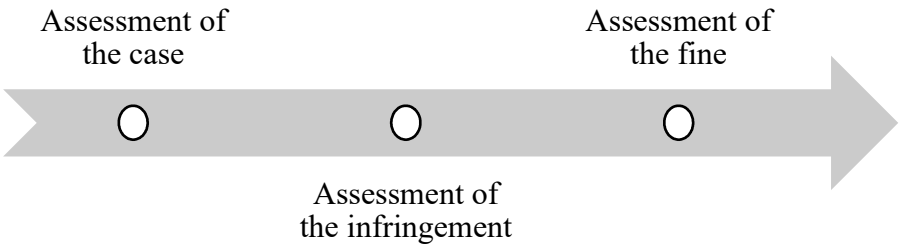

Figure 3. Evaluation procedure: three steps to determine the fines.

In the first step the facts of the case are investigated by the DPA. The aim of this step is to understand and determine more precisely what has happened. The second step leads to the assessment of whether there has been an infringement of the provisions. Any unlawful behaviour of a controller or processor is established in this step. The third step determines the level of fine. Preliminary to this, in the second step the type of corrective measure will be selected. Step three only applies if the corrective measure is an administrative fine. If warnings and reprimands are issued there is no need for the DPA to follow-up with step three. This conclusion is endorsed by the GDPR in Recital (148) and by the EDPB[49].

[47] Greengard, S. (2018) Weighing impact of GDPR, *Communications of ACM* 61 (11), p. 17.

[48] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p.7.

Following the completion of the first two steps, the DPAs will follow-up with the third step and determine the level of fine. Step three has a high degree of complexity and subjectivity. It is the heart of both P2 and P3. Accordingly, if the factual analysis (step 1) has prompted there has been a conflict between the behaviour of controller or processor with the legislative background, and the legal analysis (step 2) provides proof of infringement deserving an administrative fine, the amount is calculated based on eleven factors. These are discussed in sections 2.5.1. – 2.5.11.

2.5.1 NATURE, GRAVITY, AND DURATION

Embracing the GDPR spirit, all the obligations incumbent on controllers and processors are categorized according to their nature in Art. 83 (4) – (6). The nature of infringement is a result of such classification. The EDPB Guidelines are pointing towards the fact that Recital (148) opens the possibility for DPAs to issue reprimands instead of fines[50]. An example of this would be if the data controller is a natural person and the fine would constitute a disproportionate burden[51]. Here the reader may witness the evaluation procedure referenced under Figure 3. Hence, the DPAs are poised to perform case-by-case evaluations. The competent DPA during its investigation process will assess if a fine is necessary as a corrective measure. In many cases the DPAs will decide against a fine for this reason.

How gravity may be assessed is left to the discretionary power of DPAs to decide. In fact, the EDPB Guidelines provide that[52]:

> *"The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement."*

Yet the duration of infringement may be illustrative of the three scenarios provided by EDP as example, it is not always obvious and easy to determine the duration of the infringement. This is especially true in cases of personal data breaches due to cybersecurity threats. The personal

---

[49] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 9.

[50] Ibid.

[51] Ibid.

[52] *Op cit,* p. 10.

data breaches are one of the gravest infringements of GDPR, compared to the lack of Data Protection Officer's (DPO) contact details in the information notice. Personal data breaches are responsible for most damages suffered by data subjects and often involve the highest number of impacted data subjects. It is a top priority for organizations to evaluate and understand the source of the personal data breaches. It could be a challenge to recognize these, however there are numerous examples provided by both academia and practice. Once recognized, the root-cause for personal data breaches should be determined. There is a need to understand the causal link between a certain human error, a process, a procedure or an entire policy and the personal data breach itself. Once the root-cause analysis provides its results, competent key-personnel should conduct the treatment plan to mitigate the negative effects of personal data breaches.

Due to the argument presented above, DPAs should investigate the number of data subjects involved, the purpose of the processing and the compatible use[53] and if the data subjects have suffered damage[54].

2.5.2 INTENTIONAL OR NEGLIGENT CHARACTER

The EDPB Guidelines provide examples of both intentional breaches and infringements resulting from negligence[55]. The GDPR highlights, and endorsed by interview subjects, that all data processing routines are following a risk-based approach. This approach requires constant evaluation, measuring, adaption and performance review. It is an infinite loop meant to be interpreted as an obligation of goal rather than an obligation of mean. Thus, neither controllers nor processors are permitted to legitimize infringements due to lack of resources or a imple failure to efficiently apply internal policies.

In practice organizations often avoid responsibilities due to the general perception that internal policies are only formal documents. Reality cannot be farther from that. The policies adopted in any organization serve

[53] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, (WP 203, 00569/13/EN) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 2 February 2021].

[54] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], pp. 9-11.

[55] *Op. cit*, p. 12.

the purpose to lead the way or to pave the corridors of a law-abiding behaviour. Policies can often get complicated, but the solution is to enact a "policy task force", which has its primary goal to translate it into everyday practice. Policies, i.e. documents regulating data processing activities, shall not be reactive, but proactive instead. This conclusion is supported by the idea that it is better to treat the disease not just the symptoms.

2.5.3 ACTIONS OF CONTROLLER OR PROCESSOR

There is no bulletproof system or organization. Data breaches will occur. It is not a matter of a condition, but rather of time. Controllers and processors have clear responsibilities to implement measures ensuring data security. The EDPB provides that[56]:

> *"However, when a breach occurs and the data subject has suffered damage, the responsible party should do whatever they can do in order to reduce the consequences of the breach for the individual(s) concerned. Such responsible behaviour (or the lack of it) would be taken into account by the DPAs in their choice of corrective measure(s) as well as in the calculation of the sanction to be imposed in the specific case."*

Organizations shall find actions that are suitable to provide proof of good-faith collaboration with other entities in case of infringements. Actions include reaching out to other entities involved in the data-sharing ecosystem or even restricting and blocking access to data.

2.5.4 DEGREE OF RESPONSIBILITY

This criterion from the entire framework set by Art. 83 (2) is probably the most subjective one. Just by simply reading it from the legislative text will not shed light on its practical relevance. The reference to Art. 25 and 32 of GDPR is reiterating the above presented remark that it is about the risk-assessment. Organizations are expected to have clear methodology on how to identify and assess risks. The degree of responsibility may be measured by a verification of existing documentation that was incumbent on the controller. Further, even the documentation might not suffice, if it is not followed by implementation of measures.

The EDPB Guidelines are calling for "appropriate conclusions"[57]. The DPAs will assess when the degree of responsibility has to be

[56] Ibid.

[57] *Op. cit*, p.13.

established if the controller acted based on the appropriate conclusions. Remarkably, the words "degree of" could have been deleted from the original text due to its capability to enlarge the "grey area". To what degree are one controller's assessments and measures good enough, or even compliant enough, has its own relativity. If the authority is entitled to establish the degree by itself, it has huge implications. In practical terms this means that a DPA might say that a controller's compliance efforts are not good enough and issue an administrative fine. This can lead to a depressing pressure on businesses, as budget allocations might differ from one another, as well as the place of compliance matters in the priority list.

2.5.5 PREVIOUS INFRINGEMENTS

The DPAs will keep a track record of the controller or processor committing the infringement. There is a clear intention to consider recidivism as an aggravating factor[58]. According to the EDPB Guidelines, the DPAs should assess if the controller or processor has committed the same infringement before; or if the controller or processor has committed an infringement of the Regulation in the same manner[59].

Committing the same infringement should indicate a heavier corrective measure or higher fine. Controllers or processors receiving any corrective measure from a DPA should take its implementation seriously and with utmost importance. If the same incident should happen again, it would be hard to efficiently argue against the setting of an administrative fine. On the other hand, the DPAs might incur difficulty in reaching the controller or processor. Inability to cooperate is left to be a separate benchmark in this criteria framework. However, if this is the case, a question would arise as to whether insufficient cooperation would consist of a first infringement? The utility of the question comes into discussion because in such a scenario these criteria would be fulfilled in one time. However, this interpretation is de facto detrimentally towards the controllers and processors. It would assume a recidivism by default

[58] Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under GDPR, [online]. Available from: https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr [Accessed 20.01.2021], p. 108.

[59] Article 29 Data Protection Working Party, Guidelines on application and setting of administrative fines for purposes of Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 14.

in case a controller or processor is not willing to answer to notices received from DPAs. In exchange, the insufficient cooperation would definitely constitute an aggravating factor for any "first-timer" offenders.

2.5.6 COOPERATION WITH DPAS

This criterion emphasizes the procedural part of the entire investigation process around an infringement. The DPA will engage in a dialogue with the offender in order to better understand the circumstances of the situation. A high degree of cooperation would mean that throughout the entire investigation process the controller or processor is providing clear, accurate and transparent information. It does not seek to shy away from the retaliation it might face from the DPAs, nor does alter or modify results of its assessments in such a way to bend the reality in its favour. The EDPB Guidelines are claiming the cooperation obligation to be „due regard" and arguing that it does not include any cooperation that is already required by the law (e.g. allowing access to the controllers' premises to carry out audits or inspections)[60].

2.5.7 CATEGORIES OF PERSONAL DATA AFFECTED

This criterion is related to the type of personal data that was affected by the infringement. The GDPR recognizes three major categories of personal data:

2.5.7.1 PERSONAL DATA

The DPD, the ancestor of GDPR, never intended to apply to all kinds of data. Most probably the intention was to exclude anonymized data[61] from the regulation, as this could be construed as contrary to its scope, *i.e. to offer protection only for data which can be related to a person*[62].

In 2007 the Article 29 Working Party, established under Article 20 of DPD, produced an opinion on the concept of 'personal data' to provide guidance contributing to the uniform application of data protection rules

---

[60] Ibid.

[61] Ohm, P. (2010) Broken Promises of Privacy: Responding to Surprising Failure of Anonymization, *UCLA Law Review Vol. 57*. Available from https://ssrn.com/abstract=1450006. [Accessed 11 February 2021], p. 1738.

[62] The Article 4 Par. (5) of GDPR, clarifies the aspect in question by stateing that pseudonymization' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. From the wording of Recital (28) and (78) it should be concluded that pseudonymization is encouraged by the GDPR.

across the EU. There were some important points, which should be noted since it was proposed not to fall victim of 'unduly restriction' of interpretation of personal data definition. What might have been interpreted as an over-broad application of the DPD, resulting from wide interpretation of the definition, should be balanced out by using the flexibility allowed in the time actual application of the DPD's rules.

Perhaps, EU lawmakers wanted to strike a balance through the power of technology and escalating digitalization, but all that has failed earlier then everybody expected. For this reason, a new set of rules is taking place from the next year, and reform is happening at this moment in the field of data protection. *For example, in case of* IP addresses, there was a significant divergence on the level of national regulations. The Commission's Impact assessment results prove that there have been serious differences on this topic in the recent past. For instance, only a few Member States have taken a clear regulatory approach assessing the status of IP addresses. Austria considered IP addresses as being personal data in the Austrian Security Policy Act. Laws in Cyprus, Italy and Luxembourg suggested the same, but within the context of electronic communications. According to the Bulgarian and Estonian Electronic Communications Acts, only a combined set of data which includes IP addresses constituted, as a whole, personal data[63]. Some of the Member States took the view that the processing of IP addresses does not fall within the scope of legislation implementing the Directive, as long as the addresses themselves are not linked to individuals or to PCs of individuals (e.g. Belgium, UK)[64]. The national laws of Denmark, France, Germany, Hungary, Latvia, Lithuania, Netherlands, Poland, and Spain highlighted the fact that in case where re-identification of users is possible with processing data, those data shall be considered as being personal data[65]. This is the case of IP addresses

[63] Commission Staff Working Paper of 25 January 2012, Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data of. *European Commission* (SEC (2012) 73 final). Available from https://www.europarl.europa.eu/cmsdata/59702/att_20130508ATT65856-1873079025799224642.pdf, [Accessed 11 February 2021], p. 14.

[64] Ibid.

[65] *Op cit*, p.7.

too. Besides, Austria was the first to recognise dynamic IP addresses as personal data.

This approach was embraced by the Court of Justice of European Union, regardless if the IP data are static or dynamic[66]. A dynamic IP address changes each time there is a new connection to the internet. Unlike static IP addresses, dynamic IP addresses do not enable a link to be established, by means of files accessible to the public, between a specific computer and the physical connection to the network used by the internet service provider. Therefore, only the internet service provider has the additional information necessary to identify the user. They identify a computer, not the person using it. True. But that is the same as a telephone; just because a call was made from a number does not tell you exactly who was talking[67]. And should there be a difference between the nature of an IP address and a telephone number? Probably most of the people believe their phone number is quite personal, whereas the same level of personality and/or confidentiality shall apply to an IP address too.

In this regard, the answering to the question raised by the *Bundesgerichtshof* (Federal Court of Justice, Germany), the Court of Justice of the European Union states: 'that a dynamic IP address registered by an 'online media services provider' (that is by the operator of a website, in the present case the German Federal institutions) when its website, which is accessible to the public, is consulted, constitutes personal data with respect to the operator if it has the legal means enabling it to identify the visitor with the help of additional information which that visitor's internet service provider has[68].

Moreover, by its case-law, European Union's Court of Justice will introduce new categories, while in the fast phased modernizing society it is almost a certain fact that new types of data through which an individual could be identified will appear in a relative short period of time. Hopefully, competent bodies will decide upon this, and more than that, the informational society is ready to face technical innovations on every

---

[66] Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779, paragraph 16.

[67] Hansell, S. (2008), *Europe: Your I.P. Address Is Personal*., [blog entry], 22 January 2008, BITS. Available from: https://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/ [Accessed 17 January 2021].

[68] Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779, paragraph 49.

level. These regulations will not be adopted as slowly as it was the ongoing situation regarding the DPD.

In addition, it can be deducted, that this new tendency to sort more categories as personal data, suggests the fact that the concept cannot be treated as a strictly and promptly defined term. With the passage of time, it is very possible, if not doubtless, that the concept of personal data will be enriched with additional terms, expanding the applicability of GDPR and other acts on wider area.

Another interesting novelty is the manner in which processing can be conducted according to the GDPR, *i.e.* by structuring data. Data structuring, in essence, has to do with a system where seemingly random, unstructured data can be taken as input and a number of operations executed on it linearly or non-linearly. These operations are meant to analyse the nature of the data and its importance in the larger scheme of things. This is specifically referring to the concept of Big Data, which means extremely large data sets that may be analysed computationally in order to reveal business trends, patterns, correlations related to human behaviour through analysis of both personal and non-personal data collected from the users. As mentioned by the doctrine, the concept of Big Data, understood as a more powerful form of data mining, challenges the privacy laws in several ways, undermining the informed choice of individuals and clashing with data minimization[69]. Among the advantages of Big Data and these modern ways to use some predictive and behavioural analytics, could be mentioned the possibility to prevent diseases, efficiently combat crimes and terrorism, reduce traffic jams, and enforce new technologies in order to boost medical preventions in emergency situations. Shortly, but firmly it can be applied on various fields of life.

To state the obvious, the utility of Big Data is beyond any question, but the manner in which such analytics are being conducted by enterprises, do lead to several infringements upon privacy rights of the individuals. Firstly, given the fact, that businesses are not able to exactly determine what kind of revelations will be revealed from the examination of the data sets, any kind of consent received from the customers should be considered invalid.

---

[69] Rubinstein, I. (2012) Big Data: The End of Privacy or a New Beginning? *NYU School of Law, Public Law Research Paper No. 12-56*. Available from http://dx.doi.org/10.2139/ssrn.2157659 [Accessed 17 December 2020].

Users with average knowledge and limited knowledge on internet protocols and/or privacy policies could be easily tricked into giving their consent to something that they do not understand by default. Moreover, there is no incentive to learn about the procedure which stands behind their consent, which was given by them apparently with the full awareness of all the facts, i.e. an *informed consent*. Thus, when the consent is required for processing, it cannot be stated that the organization assumed an obligation of means to facilitate all possible attempt to achieve a certain result, without committing itself to the result expected. The opposite is correct. The obligation assumed by organizations in this situation shall be classed as an obligation of goal that is to achieve a specific result, *i.e.* not to collect and analyse personal data of the users without an existing prior consent. In actuality, such data sets include enormous quantity of data. In order for businesses to have access to useful material, it is a certainty, that more personal data are being processed about the individuals than it would be necessary. Thus, data minimization is also left behind in order for Big Data analytics to prevail.

2.5.7.2 SENSITIVE DATA

The special categories of personal data are listed in art. 9 (1) of GDPR. There is a general prohibition on the processing of such personal data. The GDPR and member state laws are regulating the exceptional cases when processing is permitted.

2.5.7.3 CRIMINAL DATA

According to art. 10 of GDPR, *processing of personal data relating to criminal convictions and offences, or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority*. From this provision personal data elements like criminal convictions, criminal offences, background checks can be extracted.

2.5.8 BECOMING AWARE OF THE INFRINGEMENT

The EDPB Guidelines distinguish between five different manners by which a DPA might become aware of an infringement. It can be a result

of investigation, complaints, articles in the press, anonymous tips, or notification by the data controller[70].

It is certainly noteworthy that notification is a legal obligation of controller and thus it will not translate into a mitigating factor. However, when the DPA has to assess the degree of cooperation with the controller, it will have its own weight. A good conduct by the controller in self-reporting the incident or the infringement towards the DPA can be the difference between applying a reprimand or setting an administrative fine as a corrective measure.

2.5.9 PREVIOUS ORDERS FROM AUTHORITY

In the event previous orders such as corrective measures have been issued by the DPAs with regard to the same subject matter, this criterion comes into play. It is not referring any previous infringements by the controller or processor of any type. Instead, what the DPAs should look at is whether the organization was cautious enough to implement the measures and ensure compliance with these, in case the DPA was to levy penalties of this type on them[71].

2.5.10 CODES OF CONDUCT OR OTHER CERTIFICATIONS

This aspect is widely overlooked in practice. The approved codes of conduct and certification mechanisms are not used to their maximum potential. Yet, the EDPB argues that such a variable should be considered for the fine calculation. More precisely[72]:

> *"Where the controller or processor has adhered to an approved code of conduct, the supervisory authority may be satisfied that the code community in charge of administering the code takes the appropriate action themselves against their member, for example through the monitoring and enforcement schemes of the code of conduct itself. Therefore, the supervisory authority might consider that such measures are effective, proportionate, or dissuasive enough in that particular case without the need for imposing additional measures from the supervisory authority itself. Certain forms of sanctioning non-compliant behaviour may be made through*

[70] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 15.

[71] Ibid.

[72] Ibid.

the monitoring scheme, according to article 41 (2) c and 42 (4), including suspension or exclusion of the controller or processor concerned from the code community. Nevertheless, the powers of the monitoring body are without prejudice to the tasks and powers of the competent supervisory authority, which means that the supervisory authority is not under an obligation to take into account previously imposed sanctions pertaining to the self-regulatory scheme."

2.5.11 OTHER FACTORS

The final stage, according to the criteria framework provided by Art. 82 (3) of GDPR, the DPAs may consider any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement[73].

Surprisingly, this criterion is at the bottom of the framework list, but in practical terms it has strong importance level. Any organization can take profits from infringements of law. Administrative or penal fines are only issued if the offender is caught. Economic gains cannot be the result of illegitimate conduct. The application of an administrative fine by the DPAs should be logical consequence in case the organization is clearly profiting of the infringement.

3. FINE CALCULATION MODELS

A couple of DPAs already published their own guidelines on setting administrative fines. The message is clear towards controllers and processors: fines are on their way. In this section four calculation models are presented: 3.1 Dutch model; 3.2 British model; 3.3. German model; 3.4. Custom model.

3.1 DUTCH MODEL

On 14 March 2019, the Dutch DPA (*Autoriteit Persoonsgegevens*) has published its own Guidelines on Administrative Fines 2019[74]. The approach implemented by the Dutch DPA is a categorization of GDPR infringements into four categories. Based on Art. 2.3 of the Dutch Guidelines, these are

[73] *Op cit*, p. 16.

[74] Boetebeleidsregels Autoriteit Persoonsgegevens (2019) *Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van bestuurlijke boetes* [online] Available from: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan [Accessed 14 March 2021].

presented in Table 2. Art. 2.4 further provides that the amount of the basic fine is set at the minimum of the bandwidth plus with half the bandwidth of the fine category associated with a violation.

Category	Fine bandwidth	Standard amount:
Category I.	Fine bandwidth between €0 and €200,000	Basic fine: €100,000
Category II.	Fine bandwidth between €120,000 and €500, 000	Basic fine: €310,000
Category III.	Fine bandwidth between €300,000 and €750, 000	Basic fine: €525,000
Category IV.	Fine bandwidth between €450,000 and €1,000,000	Basic fine: €725,000

Table 2. Categories of fines applied by Dutch DPA.

According to expert practitioners[75]:

> *"Each category is linked to a specific bandwidth that the Dutch DPA considers to be "appropriate and required". This means that the fining bandwidth is considered by the Dutch DPA to be proportional on the one hand and sufficiently dissuasive for both the offender (special prevention) and other potential offenders (general prevention) on the other. Within the chosen bandwidth the Dutch DPA has determined a standard penalty which will be the "starting point" for the calculation of the fine.*
>
> *[…]*
>
> *In case of a repeat offence the fine will automatically be increased with 50% unless this would be disproportionate in the circumstances of the case. Under the Guidelines there is a repeat offence "when at the time the offence was committed there were not yet five years passed since the imposition of an administrative fine by the Dutch DPA on the offender in respect of the same or a similar offence committed by the offender". Given this*

[75] Steenbruggen, W. and Van Der Eijk, B. (2019) *Dutch regulator publishes guidelines for the calculation of administrative fines under the GDPR* [online]. Available from: https://www.twobirds.com/en/insights/2019/netherlands/dutch-regulators-publishes-guidelines-for-the-calculation-of-administrative-fines-under-the-gdpr [Accessed 15 March 2021].

definition, other measures such as warnings, reprimands or orders under penalties will not trigger a qualification as repeat offence."

The same experts highlight two points. First they argue that the bandwidths and standard penalties are much lower than the maximum amount foreseen in the GDPR, which indicates that the Dutch DPA will normally not apply the high penalty maximums of the GDPR.[76] Second, it is further debated that there is no room for turnover based fines in normal cases when it comes to fining practices of Dutch DPA.[77] Certainly, the Dutch Guidelines are not disarming the authority from the possibility to issue even maximum amount penalties or turnover based fines, however the Dutch DPA seems to recognize the challenge to translate the turnover into fine and render the economic impact of the latter on the relevant turnover.

3.2 BRITISH MODEL

The Information Commissioner's Office in the UK (the "ICO") has published for consultation its draft statutory guidance on setting the administrative fines (hereinafter "ICO Guidelines"). The ICO also provides that the final version will be released after the UK has left the EU and due changes will be considered. This is a huge step towards transparency in regulatory actions. Just the mere fact that yet another DPA is providing its own guidance on setting of fines, paves the path towards more clarity. Although practitioners argue there is still a large amount of discretion that the regulator can apply to adjust the fine both up and downwards, meaning that the process is not as transparent as it may at first seem[78].

The ICO is applying penalty notices in case of violations. A penalty notice is a formal document issued by the ICO (under section 155 DPA 2018) when it intends to fine an organization for a breach, or breaches, of the data protection law. The penalty notice sets out the amount the ICO intends to fine an organization and the reasons for its decision[79]. The aim

---

[76] Ibid.

[77] Ibid.

[78] Everett, M. (2020) *How to calculate a GDPR Fine – the proposed ICO way* [online]. Available from: https://www.lexology.com/library/detail.aspx?g=50cca832-df9c-4d39-b771-ed4b7485e833 [Accessed 14 March 2021].

[79] Information Commissioner's Office (2020) *Statutory guidance on our regulatory action* [online] Available from: https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf [Accessed 14 March 2021], p. 17.

pursued by the ICO in issuing penalty notices is in line with P2 and P3 set out in the EDPB Guidelines.

An interesting detail in the procedure provided by the ICO is the existence of a notice of intent (NOI), which advices the organization or individual that the ICO intends to serve them with a penalty[80]. The NOI sets out: (a) the circumstances of the breach; (b) the ICO's investigative findings; (c) the proposed level of penalty; (d) a rationale for the basis; and (e) the amount of the penalty[81]. If the organization disagrees with the NOI a negotiation process can take place between the concerned parties that includes either written or oral representations.

According to the ICO[82]:

> *"The maximum amount (limit) of any penalty depends on the type of breach and whether the 'standard maximum amount' or 'higher maximum amount' applies. The higher maximum amount is, in the case of an undertaking, 20 million Euros or 4% of turnover, whichever is higher, or in any other case, 20 million Euros. The standard maximum amount is, in the case of an undertaking, 10 million Euros or 2% of turnover, whichever is higher, or in any other case, 10 million Euros. Where a fine based on turnover exceeds the 10 or 20 million Euros limit, the ICO will cap the fine at the relevant limit. The ICO may impose a fine up to the relevant limit, if a fine based on turnover would not result in a proportionate fine because, for example, a company has a very low or no turnover (but has committed a serious breach of data protection law)."*

The overview of the nine-step evaluation process is provided in Figure 4 below. Details on each step are included in the ICO Guidelines.

[80] *Op cit*, p. 18.
[81] Ibid.
[82] *Op cit*, p. 20.

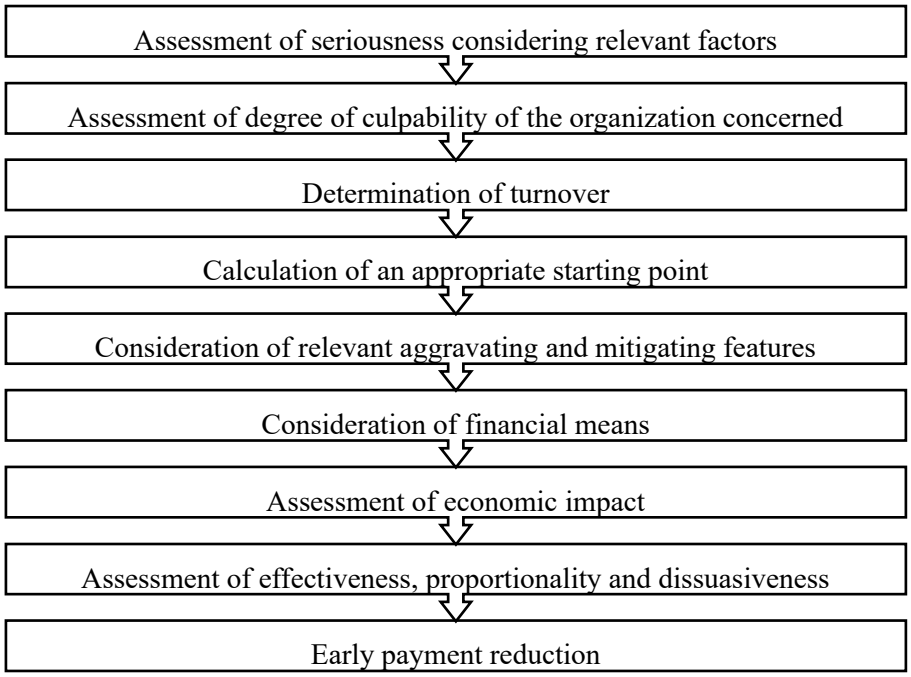

Figure 4. Nine-step evaluation process by the ICO.

Nonetheless, both the third and the last step are noteworthy points. In order to set the starting point under step three, the ICO provides a very helpful structure shown in Table 3. From the examination of this table, one may easily spot differences between the fine's bandwidths suggested by the ICO and the Dutch DPA. Also in its last step the ICO incentivizes the rapid payment of penalty notices. According to the ICO Guidelines, the ICO will reduce the monetary penalty by 20%, if they receive full payment of the monetary penalty within 28 calendar days of sending the notice[83]. However, this early payment discount is not available if a data controller or person decides to exercise their right of appeal to the First-tier Tribunal (Information Rights)[84].

[83] Information Commissioner's Office (2020) *Statutory guidance on our regulatory action* [online] Available from: https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf [Accessed 14 March 2021], p. 24.

[84] Ibid.

Penalty starting point Standard Maximum Amount (SMA) (max of 2% or 10 Million Euro) Higher Maximum Amount (HMA) (max of 4% or 20 Million Euro)				
Seriousness: / Degree of culpability:	Low	Medium	High	Very High
Low / No	**SMA** 0.125% **HMA** 0.25%	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.5% **HMA** 1%
Negligent	**SMA** 0.25% **HMA** 0.5%	**SMA** 0.5% **HMA** 1%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1% **HMA** 2%
Intentional	**SMA** 0.375% **HMA** 0.75%	**SMA** 0.75% **HMA** 1.5%	**SMA** 1.125% **HMA** 2.25%	**SMA** 1.5% **HMA** 3%

Table 3. ICO Penalty Starting Point

3.3 GERMAN MODEL

The Conference of the German Data Protection Authorities (DSK) has published its own model of calculating fines under the GDPR[85]. The model is strict and can lead to very high amounts. This model heavily uses the concept of undertaking, since larger companies can receive stellar amount of fines.

The process is similar to the Dutch and British models in as much as it includes classification of infringements. It is no surprise all three models are considering such a tiering system, which has its roots in the EDPB Guidelines[86]. The DSK provides a five-step procedure to calculate fines. In comparison to the Dutch and British model, this procedure focuses on the offenders not the infringement itself.

[85] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen* [online]. Available from: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [Accessed 21 March 2021].

[86] Article 29 Data Protection Working Party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, Adopted on 3 October 2017, (17/EN, WP 253) Available from: https://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889 [Accessed 1 February 2021], p. 9.

3.3.1 CATEGORIZATION OF COMPANIES

How the DSK wishes to determine the size class of each company is based on annual threshold limits. This approach highlights the economic impact that DPAs might have. Table 4 shows the size classes.

Micro, small and medium-sized companies (SMEs)						**Large companies**	
A		**B**		**C**		**D**	
Micro companies Annual turnover up to € 2m		Small companies Annual turnover of more than € 2m up to € 10m		Medium-sized companies Annual turnover of more than € 10m up to € 50m		Annual turnover of more than € 50m	
A.I	Annual turnover up to € 700,000	**B.I**	Annual turnover of more than € 2m up to € 5m	**C.I**	Annual turnover of more than € 10m up to € 12.5m	**D.I**	Annual turnover of more than € 50m up to € 75m
A.II	Annual turnover of more than € 700,000 up to € 1,4m	**B.II**	Annual turnover of more than € 5m up to € 7.5m	**C.II**	Annual turnover of more than € 12.5m up to € 15m	**D.II**	Annual turnover of more than € 75m up to € 100m
A.III	Annual turnover of more than € 1,4m up to € 2m	**B.III**	Annual turnover of more than € 7.5m up to € 10m	**C.III**	Annual turnover of more than € 15m up to € 20m	**D.III**	Annual turnover of more than € 100m up to € 200m
				C.IV	Annual turnover of more than € 20m up to € 25m	**D.IV**	Annual turnover of more than € 200m up to € 300m
				C.V	Annual turnover of more than € 25m up to € 30m	**D.V**	Annual turnover of more than € 300m up to € 400m
				C.VI	Annual turnover of more than € 30m up to € 40m	**D.VI**	Annual turnover of more than € 400m up to € 500m

	C.VII	Annual turnover of more than € 49m up to € 50m	**D.VII**	Annual turnover of more than € 500m

Table 4. Determination of size class.

3.3.2 AVERAGE ANNUAL TURNOVER

These are determined based on DSK guidance. Table 5 presents the thresholds of average annual turnovers.

Micro, small and medium-sized companies (SMEs)						Large companies	
A		B		C		D	
A.I	€ 350,000	**B.I**	€ 3.5m	**C.I**	€ 11.25m	**D.I**	€ 62.5m
A.II	€ 1,050,000	**B.II**	€ 6.25m	**C.II**	€ 13.75m	**D.II**	€ 87.5m
A.III	€ 1.7m	**B.III**	€ 8.75m	**C.III**	€ 17.5m	**D.III**	€ 150m
				C.IV	€ 22.5m	**D.IV**	€ 250m
				C.V	€ 27.5m	**D.V**	€ 350m
				C.VI	€ 35m	**D.VI**	€ 450m
				C.VII	€ 45m	**D.VII**	concrete annual turnover*

* If the annual turnover exceeds € 500m, the maximum fine of 2% or 4% of the annual turnover must be taken as the maximum limit, so that the calculation is based on the actual turnover of the respective company.

Table 5. Average annual turnover rates.

3.3.3 DAILY RATES

The daily rates are calculated using a simple mathematical calculation. The average annual turnover rates are divided by 360. Table 6 provides the overview of daily rates.

Micro, small and medium-sized companies (SMEs)						Large companies	
A		B		C		D	
A.I	€ 972	**B.I**	€ 9,722	**C.I**	€ 31,250	**D.I**	€ 173,611
A.II	€ 2,917	**B.II**	€ 17,361	**C.II**	€ 38,194	**D.II**	€ 243,056
A.III	€ 4,722	**B.III**	€ 24,306	**C.III**	€ 48,611	**D.III**	€ 416,667
				C.IV	€ 62,500	**D.IV**	€ 694,444
				C.V	€ 76,389	**D.V**	€ 972,222
				C.VI	€ 97,222	**D.VI**	€ 1.25m
				C.VII	€ 125,000	**D.VII**	concrete daily rate*

* If the annual turnover exceeds € 500m, the maximum fine of 2% or 4% of the annual turnover must be taken as the maximum limit, so that the calculation is based on the actual turnover of the respective company.

3.3.4 DAILY RATES MULTIPLIED BY FACTORS.

In order to receive the final amount, the daily rate has to be multiplied by a factor. This factor is based on the degree of severity of infringement and whether it is a formal or material offence. Formal infringements are listed in Art. 83 (4) of GDPR, while material offences are the ones provided by Art. 83 (5) and (6) of GDPR. The factors are displayed in Table 7.

Degree of severity of offence	**Factor for formal offences**	**Factor for material offences**
Light	1 to 2	1 to 4
Medium	2 to 4	4 to 8
Severe	4 to 6	8 to 12
Very severe	6 <	12<

Table 7. Factors applied to daily rates.

3.3.5 FINE ADJUSTMENT

This last step pinpoints the fact that the amount calculated will be adjusted on the basis of circumstances in favour of and against the party concerned, as far as these have not yet been taken into account in the fourth step. In particular, this includes all offence-related circumstances (cf. catalogue of criteria in Art. 83 para. 2 GDPR) as well as other circumstances, such as a long proceeding or an imminent company insolvency[87].

Ziegler and Eichelmann argue that the above five steps can be summarized in a general formula[88] described as the average annual turnover divided by daily rates and then multiplied by factors, where the amount received is subject to substantial scrutiny of the competent DPA.

Hamelin and Brandt heavily debate the legal conformity of the German model. They argue that there is a dubious reference to 'group turnover'[89]. As the authors provide it[90]:

---

[87] Ziegler, S. and Eichelmann, A. R. (2019) *Five steps to calculate GDPR fines: new model adopted by German data protection authorities conference* [online]. Available from: https://www.herbertsmithfreehills.com/latest-thinking/five-steps-to-calculate-gdpr-fines-new-model-adopted-by-german-data-protection [Accessed 16 March 2021].

[88] Ibid.

[89] Hamelin, A. and Brandt, E. (2019) *The German model for calculating fines under GDPR: more questions than answers* [online]. Available from: https://technologyquotient.freshfields.com/post/102fvyu/the-german-model-for-calculating-fines-under-gdpr-more-questions-than-answers [Accessed 16 March 2021].

[90] Ibid.

> *"According to Article 83 of the GDPR – the key provision on fines – the reference point for the fine is 'the undertaking', not 'undertakings' or 'a group of undertakings. This suggests the legislator intended that a fine would apply to the particular infringing business rather than the wider group.*
>
> *This makes even more sense when considering that GDPR infringements may only be committed by a data controller or processor acting as a single entity. Why then should fines be determined on the basis of the group turnover, which would include entities that are not involved in the data processing?*
>
> *Furthermore, this competition law-like approach does not fit the GDPR system. Under competition law, fines are calculated based on group turnover to account for the fact that the parent company might have benefited from the infringement. This does not necessarily apply to GDPR infringements, which do not always result in commercial benefits for the controller or processor."*

Further, practicing lawyers share the concerns on legitimacy of this model. Wybitul and Crawford provide that[91]:

> *"Whether sanctions imposed under the DSK fine model properly take into account the criteria required by Article 83 GDPR or can properly ensure that fines are in fact proportionate, is questionable. The DSK model, if adopted and applied, would be ripe for challenge. It could be difficult for data protection authorities to convince courts in administrative offence proceedings that the authorities in fact have determined appropriate, lawful fines using the model."*

As a conclusion to the German model, the strong opposition is caused because such a fining model would lead to the brutal application of a stick and carrot approach. Eventually, what the German DPAs aim to achieve is to apply the possibilities offered by the GDPR. This was that personal data protection can grow not only teeth, but claws as well. It should not

[91] Wybitul, T. and Crawford, G. (2019) *German Data Protection Authorities Adopt New GDPR Fine Model* [online]. Available from: https://www.jdsupra.com/legalnews/german-data-protection-authorities-38441/ [Accessed 17 March 2021].

be a paper tiger anymore, but a reckoning force that has to be feared. The German DPAs are right about this. They should be feared because they regulate a piece of legislation that is connected to a fundamental right: the right to privacy.

In chronological order the German model was among the first to be announced. Due to its rigorous approach, it had quite a wide reach in both academia and practice. There are notable attempts to reconstruct the model and translate it into GDPR fine calculators. By way of example, Cristopher Schmidt created such calculators[92], CMS Tax Law[93] and by Compliance Essentials GmbH[94]. The last GDPR fine calculator manages to synthetize in the most efficient way the steps presented above.

3.4 CUSTOM MODEL

In addition to the guidelines issued by DPAs, academia has provided its own point of view in relation to the setting of administrative fines. A holistic view is applied by Maxwell and Gateu in saying that the tiering systems applied by EDPB does not provide a reliable benchmark for assessing nature and gravity"[95]. They recommend that a more reliable proxy would be to discover the number of data subjects affected and multiply with the level of damage suffered by each of them[96]. This individual damage score may be determined – according to the authors – based on type of incidents[97]. They argue that[98]:

> *"A violation involving sensitive data, or resulting in identity theft, might correspond to a high damage score for each individual than a violation creating no damage, for example a failure to mention the duration of data retention in an information notice.*

---

[92] Schmidt, C. (2019) *GDPR Fine Calculator based upon the Fining Schedule of German DPAs* [software] v.2.1. Available from: https://app.calconic.com/api/embed/calculator/5d889ed254e7dd001eadd4ed [Accessed 20 March 2021].

[93] CMS Tax Law (2020) *Fine Models by DPAs – Germany* [software]. Available from: https://www.enforcementtracker.com/?finemodel-germany [Accessed 20 March 2021].

[94] Compliance Essentials (2020) *GDPR Fine Calculator* [software]. Available from: https://www.dsgvo-portal.de/gdpr-fine-calculator.php [Accessed 20 March 2021].

[95] Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr [Accessed 20.01.2021], p. 105.

[96] Ibid.

[97] Ibid.

[98] Ibid.

(…)

For example, in the case of a data breach involving the loss of sensitive data for 100,000 data

subjects, the number of data subjects may be multiplied by a high individual damage score, for

*example 3. This would yield a nature and gravity score of 100,000 * 3 = 300,000.*

(…)

*A purpose for data processing with a high level of utility for society, e.g. medical research, might warrant a lower multiplier than a purpose with lower societal benefits, e.g. commercial advertising. In the context of our example, let us imagine that the processing of sensitive data was done for the purpose of creating commercial profiles for advertising. This would generate a high purpose multiplier, for example 3, compared to processing for medical research, which would generate a low purpose multiplier of 1. Thus in the foregoing example, the nature and gravity score would again be multiplied by 3: 300,000 * 3 = 900,000.*

(…)

In addition to the nature and gravity, the duration of the violation must also be taken into account. Adding duration to the formula is straightforward: It would be sufficient to add a multiplier to the equation corresponding to the number of months during which the violation occurred. In the above example, if the data vulnerability resulting in the loss of sensitive data lasted for 6 months, the resulting nature and gravity score (900,000) would be multiplied by 6, the number of months during which the violation occurred. A linear duration multiplier is routinely used in setting of competition law fines."

The custom model dives into and tries to bring parallels between data protection law and competition law. The authors are convinced that the above-mentioned variables are relatively easy to be calculated. From here it would also be straightforward to develop a scoring system or calculation starting points. This methodology can be seen in practice from the other models analysed in this chapter. They see the big challenge to set the initial monetary amount to correspond to each point in the score[99].

4. FINE PREDICTION ANALYSIS

In this sub-chapter, results of predictive analysis are presented. This research builds on regression models constructed in R programming language. The dataset is generated by the use of publicly available data on existing GDPR fines, as well as additional information, which was acquired in partnership with a private company. The analysis will also cover a country level case-study in section 4.5.

4.1 METADATA

The dataset includes 15 variables and 312 observations. Each observation is a case in which an administrative fine has been set for GDPR infringement. The variables used in this session are factor and double variables. Table 8 contains a description of each.

Name	Type	Description
Country	Factor	Represents the country in which the DPA has issued the administrative fine.
type	Factor	Represents the nature of infringement for which the fine has been issued.
industry	Factor	Represents the industry in which the controller or processor is acting.
tiertwo	Factor	Represents the delimitation based on the tiering system introduced by the GDPR. If the infringed article referenced by the DPA is mentioned in Article 83 (5) of GDPR, it will be qualified as a higher infringement, otherwise if it will remain a minor infringement for which Article 83 (4) of GDPR applies.
Fine	Double	The amount of monetary sanction given to the controller or processor

[99] *Op cit*, p. 111.

article	Double	The number of articles referenced by the DPA in the communication.
calc	Double	The number of months passed since the GDPR is applied.
calc2	Double	The number of days passed since the GDPR is applied.
turnover	Double	The amount of turnover realized by the controller or processor in 2019.
employee	Double	The number of employees of the controller or processor in 2019.
age	Double	The company seniority level that is calculated by subtracting the date of establishment from the current year.
keyarticle	Factor	It is used to verify if Article 25 or 32 is referenced by the DPA in the communication about the fine. This variable aims to verify the degree of responsibility as recommended by the EDPB Guidelines.
track	Factor	It is used to verify if the controller or processor has committed any previous infringements of GDPR. The presumption is that if an entity appears more than once in the database, the track record should be positive.
special	Factor	It is used to verify if Article 9 or 10 is referenced by the DPA in the communication of the fine. These two articles are providing for special categories of personal data.
order	Factor	It is used to verify if Article 58 is referenced by the DPA in the communication of the fine. This article provides the DPA the possibility to issue orders towards the controllers and processors. If such orders were issued and not implemented by the controllers or processors, the order variable should be positive.

Table 8. Description of variables.

4.2 REGRESSION TREE

A regression tree is generated using specific variables. The only variable that is eliminated from this analysis is the 'Country' variable due

to the massive diversity it creates in the plot. The regression tree shows that the turnover and the number of days passed since the application of GDPR are the strongest predictors that influence the amount of a GDPR fine. The type of infringement and the industry in which the controller or processor is acting will have also significant impacts. The overall regression tree is presented in Figure 5. Unfortunately, the regression tree also shows no strong correlations between the predictors.

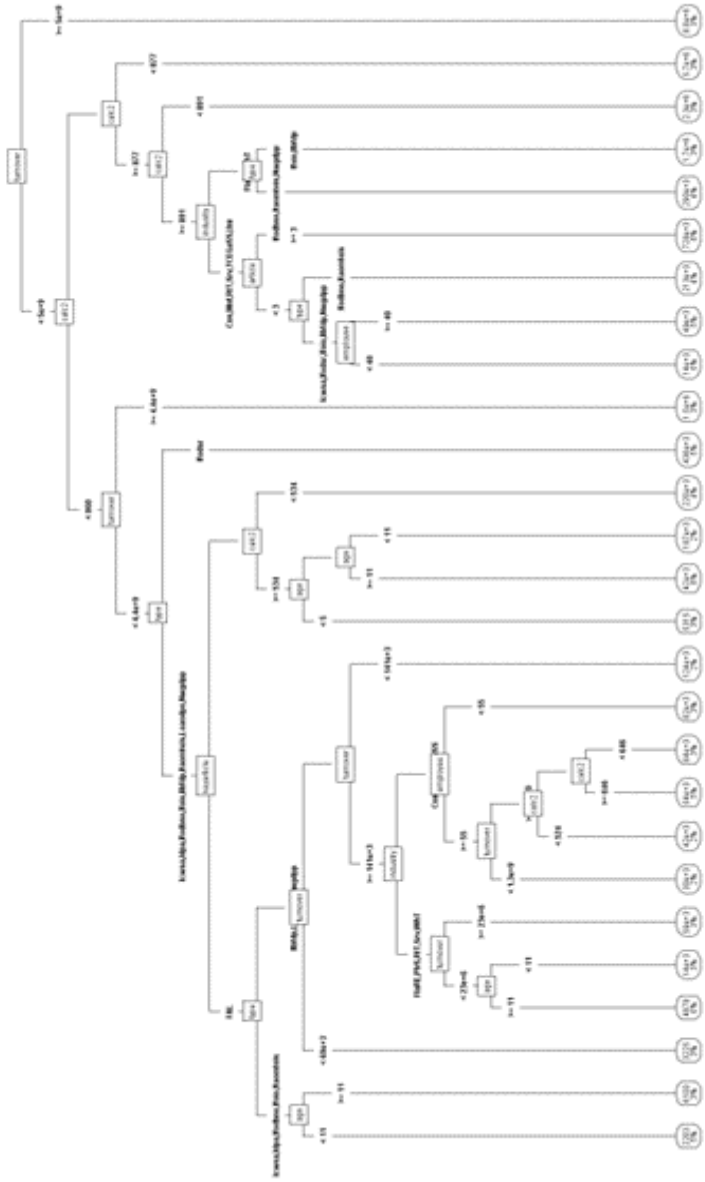

Figure 5. Regression tree of GDPR fines

4.3 RANDOM FOREST

A random forest prediction algorithm is constructed with the use of all variables. By setting the number of regression trees in this model to 1000, the error rate of the prediction model should be reduced. Figure 6 depicts the importance of variables used in this model, while Figure 7 presents the number of trees in correlation to the standard error.

Figure 6. Importance of variables plot.

The importance of variables plot explains that 'Country' and 'turnover' are two variables with the highest impact on the predicted GDPR fine. On number of trees vs standard error plot we can see that the standard error for the formula decreases in the beginning by adding new random trees to the model, however it slowly stabilizes after 200 regression trees are added to the forest and fluctuates in an insignificant manner up until 1000 regression trees are added to the forest.

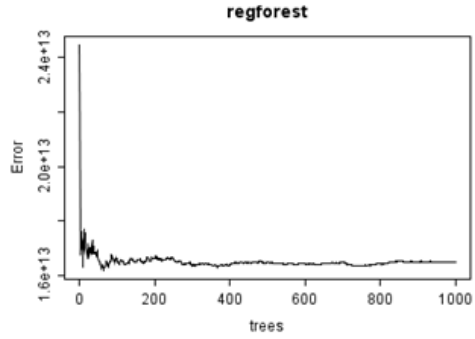

Figure 7. Number of trees vs standard error.

Further the multi-way importance plot presented in Figure 8 provides additional insights on which variables contribute the most to the accuracy of this regression model.

Figure 8. Multi-way importance plot.

4.4 LINEAR REGRESSION

The linear regression model provides poor results with no correlation between the predictors. The multiple R-squared is at 0.3736, the adjusted R-squared is sitting at 0.2648. This means that the variables used for this model are not the most accurate ones. After applying the backward variable selection, we arrive to at the conclusion that Country, article, turnover, age, and track variables should be used. However, the problem persists as the multiple R-squared value is still very low. The parameters after backward variable selection are:

Residual standard error: 3439000 on 288 degrees of freedom Multiple R-squared: 0.3473, Adjusted R-squared: 0.2952 F-statistic: 6.663 on 23 and 288 DF, p-value: < 2.2e-16

Figure 9 illustrates the impact of variables in plots. Interpretation shows that in the United Kingdom (UK) the fines can be much higher compared to the others. Also, the GDPR fines tend to increase if more articles are referenced by the DPAs in their decision to issue an administrative fine. Further, whenever the turnover number is higher for a controller or processor, the amount fined will also be higher. Moreover, the seniority level of the company is not an aggravating circumstance, in terms that more recently established companies can receive higher fines. Finally, there

is a decrease in the amount if fine, in the event a company has a track record of any previous infringement. Although this might seem an unrealistic scenario, it can be applied due to the fact that the authority considers that the controller or processor was already subject to a penalty. Nonetheless, the difference between having a track record in any previous infringement seem to be negligible from the analysis.

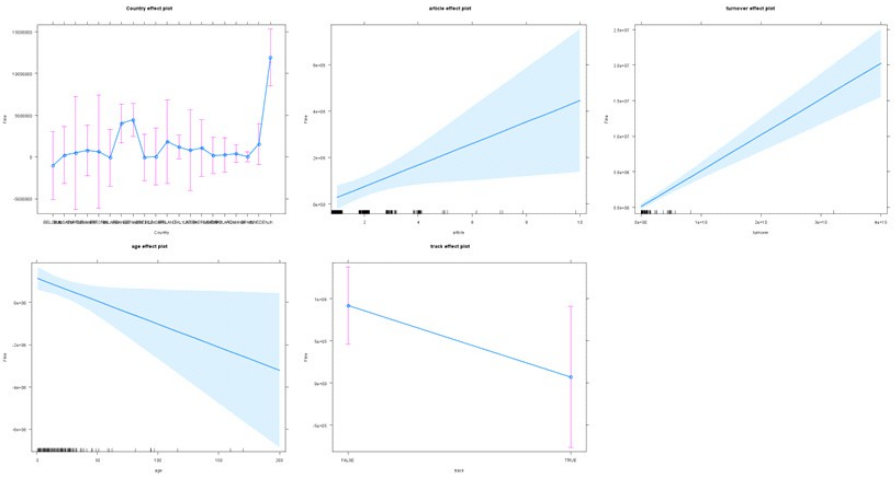

Figure 9. Impact of variables plots.

4.5 COUNTRY LEVEL ANALYSIS

The same prediction models can be performed on a different dataset. This is possible due to reporting practices of the Romanian DPA, which consistently issue a short description of the circumstances around their fining practices. By reviewing the descriptions, there is a possibility to extract new variables, which are not known of other cases. Therefore, in this sub-chapter the aim is to carry out an analysis on the Romanian cases, where a monetary sanction was applied towards a controller or processor for GDPR infringements.

4.5.1 METADATA

This dataset includes 17 variables and 40 observations. Each observation is a case officially published by the Romanian DPA. Table 9 includes a description of variables. It is worth considering that the results of the analysis will be limited to the relatively small number of observations. This will be taken into consideration throughout to process.

Name	Type	Description
months	Double	The number of months passed since the GDPR is applied.
fine	Double	The amount of monetary sanction given to the controller or processor.
type	Factor	Represents the type GDPR infringement.
controller	Factor	Represents the quality of party concerned, i.e. a controller or processor.
reference	Double	The number of articles referenced by the DPA in the communication.
ds	Double	The number of data subjects involved in the infringement.
undertaking	Factor	Represents if the party concerned is part of an undertaking or not.
private	Factor	Represents if the party concerned is an entity acting in the public or a private sector.
age	Double	The company seniority level that is calculated by subtracting the date of establishment from the current year.
turnover	Double	The amount of turnover realized by the controller or processor in 2019.
profit	Double	The amount of profit realized by the controller or processor in 2019.
cash	Double	The amount of free cash ready to be used by controller or processor.
employee	Double	The number of employees of the controller or processor in 2019.
complaint	Factor	Shows if the DPA issued the fine based on a complaint received from data subjects.
notification	Factor	Shows if the DPA issued the fine based on a notification submitted by the controller or processor.
special	Factor	Shows if Article 9 or 10 is referenced by the DPA in the communication, or there are outlier circumstances (e.g. the involved data subjects are minors).
industry	Factor	Represents the industry in which the controller or processor is acting.

Table 9. Variables of Romanian cases.

4.5.2 REGRESSION TREE

The regression tree is generated using all variables. The regression tree provides better correlation between the variables than in the previous scenario. The most important variables according to this model are the company age, the industry in which it is acting, and the number of data subjects affected by the infringement. Figure 10 provides the overview of the regression tree.

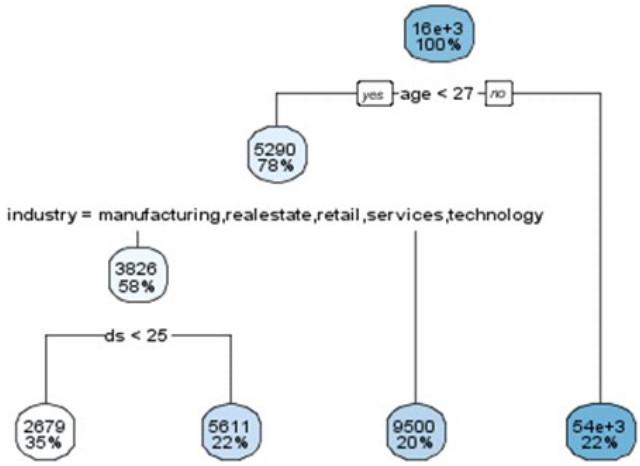

Figure 10. Regression tree of GDPR fines – Romania.

4.5.3 RANDOM FOREST

Following the example in the previous scenario, a random forest prediction algorithm is constructed with the use of all variables. The number of regression trees in this model is set to 1000 for the same reasons. Figure 12 provides the importance of variables used in this model ,m while Figure 11 presents the number of trees in correlation to the standard error.

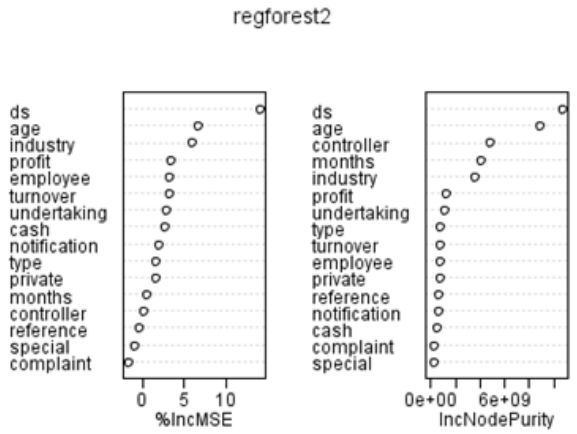

Figure 11. Importance of variables plot – Romania.

We can see that in this case the variables 'ds' and 'age' are the ones with the highest impact on the predicted GDPR fine. Similarly to the previous scenario, the standard error for the formula decreases in the beginning by adding new random trees to the model, and it stabilizes after 600 regression trees are added to the forest.

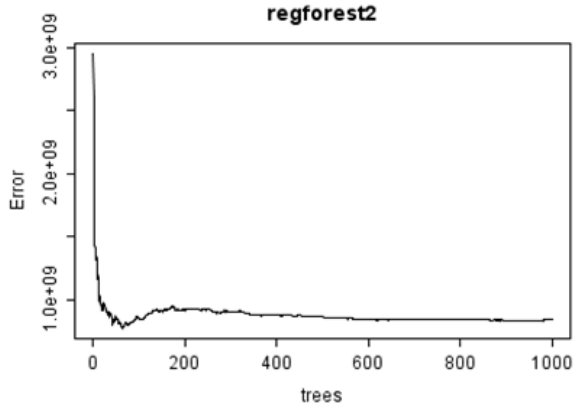

Figure 12. Number of trees vs standard error – Romania.

Also, Figure 13 gives additional insights on the multi-way importance of variables, for which the interpretation is same as in Section 4.3.

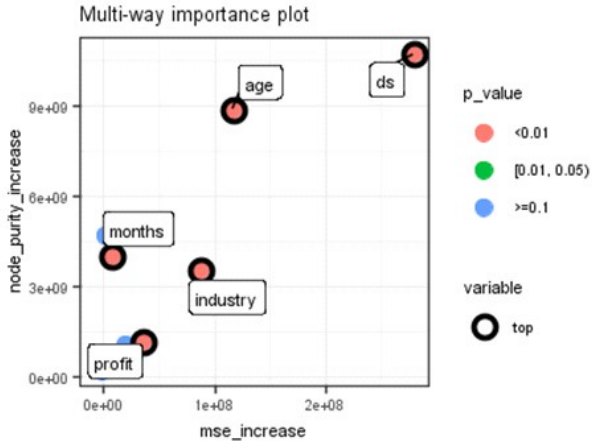

Figure 13. Multi-way importance plot – Romania.

4.5.4 LINEAR REGRESSION

The linear regression model with regards to these variables provides much better results compared to the previous dataset. The first iteration gives encouraging results, which can be presented as follows:

Residual standard error: 21920 on 14 degrees of freedom
Multiple R-squared**: 0.8573**, Adjusted R-squared: **0.6024**
F-statistic: 3.363 on 25 and 14 DF, p-value: **0.01069**

The backwards variable selection also provides guidance on eliminating at least the "months" variable, which then translate into the following results:

Residual standard error: 21180 on 15 degrees of freedom
Multiple R-squared: **0.8572**, Adjusted R-squared: **0.6286**
F-statistic: 3.751 on 24 and 15 DF, p-value: **0.005244**

The results of the effects of variables are then plotted to serve as basis of interpretation. Figure 14 provides the plot effects for each of the variables. It can be concluded that the number of data subjects involved in the data breaches is one of the most prominent variables. Second, if the DPA received a complaint, this would also entail a higher fine. Third, if the controller or processor is part of an undertaking is also an incentive to receive a higher fine. Forth, the existence of a notification to the DPA could translate into a higher fine.

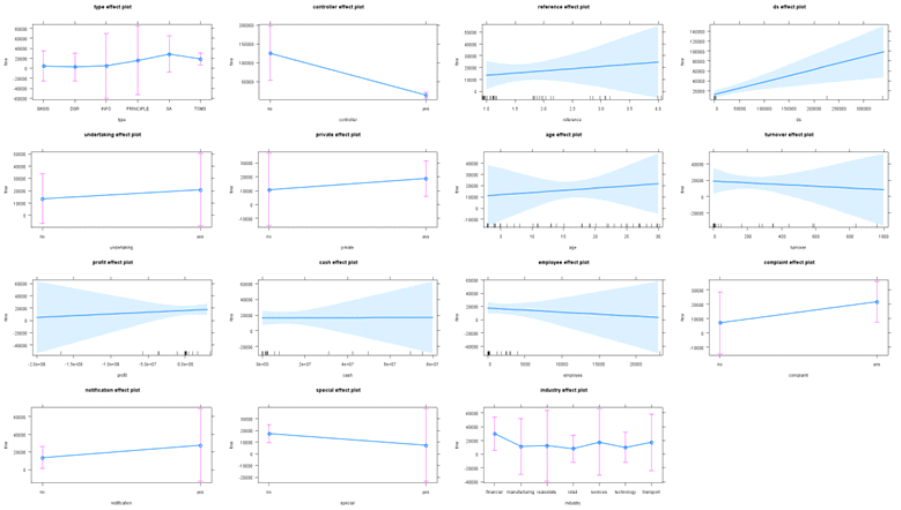

Figure 14. Impact of variables plots – Romania.

All three models are then trained with cross-validation using 15 folds with 10 repeats. The training serves the purpose to enhance the prediction accuracy. Finally the model with the most accuracy rate is selected. The regression tree as a result of cross-training got to 66%, the random forest to 69 % and the linear regression to 68 %.

The conclusion of the analysis shows that in order for these models to work more observations are needed. More observations means that more information has to be publicly available in relation to infringements. Thus, to be able to predict the amount of GDPR fines, additional information is needed for cases on the following topics as a minimum:

a. Number of data subjects affected by the infringement;
b. The existence of complaints submitted by data subjects;
c. The controller or processor forming part of an undertaking;

d. The existence of notifications submitted by the controller or processor;
e. The category of personal data involved.

5. CONCLUSION

Predicting GDPR fines is a complex topic. This subject has recently claimed the attention of academia[100]. Although arguably it is still an under-researched area. Thus, there is motivation to determine the best prediction models of GDPR fines. The motivation has multi-way implications.

First, the GDPR raises the fines thresholds. The competent authorities are entrusted to use powers given to them in this sense. This may not translate in eagerness to issue stellar amounts. If this would happen, certain industries or sectors would witness severe headwind. Yet, competent authorities should embrace the spirit of dissuasive administrative fines.

Second, the same authorities are lacking qualified personnel. In the event they decide to use regression analysis as a prediction model, it could lead to an enhanced internal workflow. The findings of an investigation would be added to the model, and a preliminary amount issued as administrative fine would then be auto-generated. Finally, human intervention by the competent authority may revise the level of fine. At the very least, it could speed up their entire process.

Third, fine calculation models presented in Section 3 vary on country level. There is no consistency, as DPAs are embarking on different roads. More clarity is needed on this level. Controllers and processors are not in the position to reasonably know what to expect. The calculators currently available based on the German model are just black box predictions. The values are not customized according to different characteristics of an entity.

This chapter identifies existing guidelines. It also presents the suggested calculation models. Finally it offers a different approach to calculate fines using regression analysis. Although the models did not perform on an acceptable level, the main conclusion is that this is due to lack of information on suggested variables. Nevertheless, the most optimal variables are subject to a constant evaluation procedure. Key importance

[100] Ruohonen J. and Hjerppe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, pp. 2-9. Available from http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf [Accessed 5 February 2021].

has to be provided to the nature of personal data involved in the infringements, to the categories of data subjects affected by such infringements and not at least, whether complaints have been submitted to the competent authority in a particular case. Fulfilment of notification obligation of controllers or processors is also a decisive factor. Yet, the authority has to evaluate the economic situation of each entity that is subject to investigation. The economic situation could translate in a wide-range of variables. Only turnover-based judgments might lead to wrong decisions. The fining practices of DPAs confirm this view.

The analysis and the interviews carried out in this chapter are representing a good starting point. Nonetheless, these are limited to lack of cases available for examination. Future work indicates the need to perform the regression analysis, once a better data-set can be constructed. Additional calculation models that will be published in the future by DPAs might bring researchers one step closer to understand intentions behind the curtains. The current fining practices are still overwhelmed with high degree of discretionary subjectivity. With the value of money being quite different across Europe, this is still a problem that is desperately looking for a solution.

LIST OF REFERENCES

[1] Albrecht, J. P. (2016), Privacy enforcement in search of its base, In: David Wright and Paul De Hert (eds) *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, Springer International Publishing

[2] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013, (WP 203, 00569/13/EN) Available from: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [Accessed 2 February 2021].

[3] Barrett, C. (2020) Emerging Trends from the First Year of EU GDPR Enforcement, *ABA – American Bar Association Data, Spring 2020* 16 (3). Available from https://www.americanbar.org/groups/science_technology/publications/scitech_lawyer/2020/spring/emerging-trends-the-first-year-eu-gdpr-enforcement/#25 [Accessed 25 January 2021].

[4] Blutman, L. (2014), *Az Európai Unió joga a gyakorlatban*, Budapest, HVG-ORAC, p.158. .

[5] Boetebeleidsregels Autoriteit Persoonsgegevens (2019) *Beleidsregels van de Autoriteit Persoonsgegevens van 19 februari 2019 met betrekking tot het bepalen van de hoogte van*

bestuurlijke boetes [online] Available from: https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-past-boetebeleidsregels-aan [Accessed 14 March 2021].

[6] Commission Staff Working Paper. SEC (2012) 72 final, Brussels, 25.1.2012. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_en.pdf

[7] Directive (EC) 95/46 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 *Official Journal of the European Union* (L281, 23/11/1995 P. 0031 – 0050). Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046 [Accessed 4 February 2021].

[8] Everett, M. (2020) *How to calculate a GDPR Fine – the proposed ICO way* [online]. Available from: https://www.lexology.com/library/detail.aspx?g=50cca832-df9c-4d39-b771-ed4b7485e833 [Accessed 14 March 2021].

[9] Golla, S. (2017) Is Data Protection Law Growing Teeth? The Current Lack of Sanctions in Data Protection Law and Administrative Fines under the GDPR, *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law* 8 (1). Available from https://www.jipitec.eu/issues/jipitec-8-1-2017/4533 [Accessed 10 February 2021].

[10] Greengard, S. (2018) Weighing the impact of GDPR, *Communications of the ACM* 61 (11) .

[11] Hamelin, A. and Brandt, E. (2019) *The German model for calculating fines under GDPR: more questions than answers* [online]. Available from: https://technologyquotient.freshfields.com/post/102fvyu/the-german-model-for-calculating-fines-under-gdpr-more-questions-than-answers [Accessed 16 March 2021].

[12] Hansell, S. (2008), *Europe: Your I.P. Address Is Personal*., [blog entry], 22 January 2008, BITS. Available from: https://bits.blogs.nytimes.com/2008/01/22/europe-your-ip-address-is-personal/ [Accessed 17 January 2021].

[13] Information Commissioner's Office (2020) *Statutory guidance on our regulatory action* [online] Available from: https://ico.org.uk/media/about-the-ico/consultations/2618333/ico-draft-statutory-guidance.pdf [Accessed 14 March 2021]

[14] Judgement of Comet BV v Produktschap voor Siergewassen, Case C-45/76, ECLI:EU:C:1976:191.

[15] Judgement of Confederación Española de Empresarios de Estaciones de Servicio v Compañía Española de Petróleos SA, Case C-217/05, ECLI:EU:C:2006:784.

[16] Judgement of Höfner and Elsner v Macrotron GmbH, Case C-41/90, ECLI:EU:C:1991:161.

[17] Judgement of LCL Le Crédit Lyonnais v. Fesih Kalhan, Case C- 565/12, ECLI:EU:C:2014:190.

[18] Judgement of Patrick Breyer v Bundesrepublik Deutschland, Case C-582/14, EU:C:2016:779.

[19] Judgement of Ute Reindle v. Bezirkshauptmannschaft Innsbruck, C- 443/13, ECLI:EU:C:2014:2370.

[20] Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (2019) *Konzept der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Bußgeldzumessung in Verfahren gegen Unternehmen* [online]. Available from: https://www.datenschutzkonferenz-online.de/media/ah/20191016_bu%C3%9Fgeldkonzept.pdf [Accessed 21 March 2021].

[21] Maxwell, W. and Gateu, C. (2019), A point for setting administrative fines under the GDPR, [online]. Available from: https://www.engage.hoganlovells.com/knowledgeservices/news/an-approach-for-setting-administrative-fines-under-the-gdpr [Accessed 20.01.2021]

[22] Ohm, P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, *UCLA Law Review Vol. 57*. Available from https://ssrn.com/abstract=1450006. [Accessed 11 February 2021], p. 1738.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) *Official Journal of the European Union* (L 119, 4.5.2016, p. 1–88). Available from: https://eur-lex.europa.eu/eli/reg/2016/679 [Accessed 4 February 2021]

[24] Rubinstein, I. (2012) Big Data: The End of Privacy or a New Beginning? *NYU School of Law, Public Law Research Paper No. 12-56*. Available from http://dx.doi.org/10.2139/ssrn.2157659 [Accessed 17 December 2020].

[25] Ruohonen J. and Hjerppe K. (2020) The {GDPR} enforcement fines at glance, *Information Systems* 106, pp. 2-9. Available from http://ceur-ws.org/Vol-2690/COUrT-paper1.pdf [Accessed 5 February 2021].

[26] Steenbruggen, W. and Van Der Eijk, B. (2019) *Dutch regulator publishes guidelines for the calculation of administrative fines under the GDPR* [online]. Available from: https://www.twobirds.com/en/insights/2019/netherlands/dutch-regulators-publishes-

guidelines-for-the-calculation-of-administrative-fines-under-the-gdpr [Accessed 15 March 2021].

[27] UC Business Analytics R Programming Guide (2018), available: www.uc-r.github.io

[28] Wybitul, T. and Crawford, G. (2019) *German Data Protection Authorities Adopt New GDPR Fine Model* [online]. Available from: https://www.jdsupra.com/legalnews/german-data-protection-authorities-38441/ [Accessed 17 March 2021].

[29] Ziegler, S. and Eichelmann, A. R. (2019) *Five steps to calculate GDPR fines: new model adopted by German data protection authorities conference* [online]. Available from: https://www.herbertsmithfreehills.com/latest-thinking/five-steps-to-calculate-gdpr-fines-new-model-adopted-by-german-data-protection [Accessed 16 March 2021].

DOI 10.5817/MUJLT2022-2-4

PLEA OF NECESSITY: LEGAL KEY TO PROTECTION AGAINST UNATTRIBUTABLE CYBER OPERATIONS*

by

JAKUB SPÁČIL

Cyber operations represent one of the main security threats today. The number of cyber operations attacking critical infrastructure is increasing year by year and states are looking for means to defend against this threat. However, the origin of hostile cyber operations is often located in the territory of another state, and attacked states must therefore grapple with the question of international law in their search for an effective defence mechanism. If states wish to defend themselves actively, the sovereignty of another state may be infringed, and such an infringement must be justified by an instrument of international law. These instruments of international law are retorsion, countermeasures, self-defence and plea of necessity. Application of plea of necessity, unlike the other alternatives mentioned, is not premised on the attributability of the cyber operation to the state, and it is precisely the attribution of cyber operation that poses one of the main problems of taking legal defensive measures. The article is divided into two parts. The first part is devoted to the relationship between retorsion, countermeasures, self-defence and plea of necessity. The second part discusses the conditions for the application of plea of necessity in the cyber context. The text takes into account the available state practice, in particular the national positions on the application of plea of necessity in the cyber context published in the last three years.

KEY WORDS

cyber operations, international law, plea of necessity, self-defence, cyber attack, attribution of cyber operation

* The article was written as an output of the project "Action in plea of necessity as a defence against cyber operations of non-state actors" implemented under the auspices and with the financial support of the Faculty of Law of Palacký University in Olomouc.

1. INTRODUCTION

The development of information technology has been a source of unprecedented economic growth for companies and an increase in the standard of living for individuals. At the same time, however, it also brings risks. Modern societies and their survival literally depend on computer-controlled systems (water distribution, healthcare system, electricity distribution, to mention just a few). It is therefore not surprising that cybersecurity is becoming a topic of paramount importance.

States are increasingly forced to confront cyber operations that result in economic and material damage.[1] In the case of a domestic cyber operation, States generally have sufficient domestic legal means to protect themselves (for example, through law enforcement or military action). However, a problem arises when the cyber operation originates in the territory of another state. In this situation, international law and its fundamental principles, such as sovereignty, the prohibition of interference or the prohibition of the use and threat of force, come into play, which significantly limit the legal ability of the attacked state to defend itself against a cyber operation from a foreign state. The attacked state is thus forced to choose between retorsion, countermeasures, self-defense, and plea of necessity, each of which is limited by a number of conditions and varies in effectiveness.

A fundamental issue that influences considerations on the choice of an appropriate defensive measure is the question of the attributability of a cyber operation to the state from whose territory it is carried out. A distinction must be made between attribution in the legal and technical sense. Attributability of acts in the legal sense, although not free from some controversies, has already been clarified to a large extent in the work on the Draft Articles on Responsibility of States for Internationally Wrongful Acts ("ARSIWA") carried out by the International Law Commission and in the jurisprudence of international tribunals.[2]

However, attribution in the technical sense is particularly problematic. While in the case of a conventional attack it is relatively easy to determine

[1] In 2021 alone, 118 cyber incidents were recorded and classified as "significant" by the Center for Strategic & International Studies, including a ransomware attack on the Colonial Pipeline, "the largest fuel pipeline in the United States"; Center for Strategic & International Studies. (2022) *Significant cyber incidents.* [online] Washington, D. C.: CSIS. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 3 January 2022].

the place of origin of the threat by locating the place of launch of a missile or the place of launch of bombers or inferring information about the origin from the very nature of the weapon used (e. g. missiles used by a particular State), in cyberspace the situation is much more complex.

The means to carry out a cyber operation are freely available to almost anyone, just a few mouse clicks away. If it is a sophisticated cyber operation, then it usually involves masking the origin, for example by redirecting traffic through third countries. And even if the specific device from which the cyber operation was carried out can be identified, the search for the perpetrator is not over, as it may be difficult to determine who controlled the device and whether the link between that person and the state existed or was sufficiently intense to meet the requirements for legal attribution of the conduct to the State.[3]

Thus, in the case of cyber operations, it is often impossible to prove that they are attributable to another State. In such circumstances, the attacked State finds itself in a difficult situation, since attribution of the operation to a State is an element of internationally wrongful act which itself is one of condicions sin qua non for applicability of most of the circumstances precluding wrongfulness under international law. One of the few such circumstances that are applicable even in the absence of attribution (and internationally wrongful act) is the plea of necessity.[4] This is the reason why this institute has received increasing attention in recent years, not only in the scholarly debate,[5] but references to this institute are also beginning to appear in the national cyber strategies of a number of States.[6]

The aim of this paper is a detailed analysis of the plea of necessity and its applicability in the context of cyber operations. Since the plea of necessity

---

[2] International Law Commission. (2001) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two, arts. 4-11 (hereinafter "ARSIWA 2001 with commentaries"); Nicaragua v. United States of America (1986) International Court of Justice, *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, paras. 105-115 (hereinafter "Nicaragua v. United States").

[3] ARSIWA 2001 with commentaries, arts. 4-11.

[4] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 251.

[5] A comprehensive analysis of the plea of necessity in the context of cyber operations (with a focus on the use of force) is offered by Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, pp. 201-257; see also Arimatsu, L. and Schmitt, M. N. (2021) The Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, pp. 1171-1198.

has not yet been invoked by any State as a circumstance precluding wrongfulness in the cyber context, the analysis builds on state practice and case law available for different contexts and suggests ways how to apply this concept in the realm of cyber operations. The paper focuses on conditions of the plea of necessity established by international law one by one and deals with the question of how should these conditions be interpreted and respected in case the plea of necessity is invoked as a justification for protective measures against a cyber operation.

Necessity is one of the instruments of international law that allows a State acting under it to temporarily disregard its obligations under international law when necessary to protect the "essential interest" of that State.[7] The plea of necessity therefore appears to be an appropriate legal basis, for example, in a situation where a State is the victim of a cyber operation originating in the territory of another State, but it cannot be shown that the State is responsible (it is attributable to it) nor has it breached the obligation of due diligence, since the application of the plea of necessity is not premised on an internationally wrongful act of another State.[8] It is this aspect that makes the plea of necessity a suitable instrument to justify a protective measure against a cyber operation of unknown origin or carried out by a non-state actor from the territory of another state.[9]

The plea of necessity is a circumstance precluding wrongfulness (of an act of a State) and its definition can be found in Article 25 of ARSIWA. It can only be invoked as justification for an act if that act is "the only way for the State to safeguard an essential interest against a grave and imminent peril" under the condition that the act "does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole".[10] However, it can never be invoked in case "the international obligation in question excludes

[6] Six states have so far explicitly expressed their support for the plea of necessity in the context of cyber operations: the Netherlands (2019), France (2019), Germany (2021), Japan (2021), Norway (2021) and Switzerland (2021). an overview of their positions is available from: https://cyberlaw.ccdcoe.org/wiki/Plea_of_necessity [Accessed 3 January 2022].

[7] ARSIWA 2001, Art. 25 (1) (a).

[8] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2.

[9] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97., p. 1185-1186.

[10] ARSIWA 2001, Art. 25, para 1.

the possibility of invoking necessity" or if the invoking State "has contributed to the situation of necessity".[11]

It follows from this definition that the plea of necessity is available to the State only under strict conditions aimed at limiting the possibility of abuse of this instrument.[12] It is an instrument which "can only be accepted on an exceptional basis"[13] and whose threshold is extremely high.[14] the exceptional nature of the plea of necessity is also confirmed by the negative wording of this article of ARSIWA.[15] The conditions of the plea of necessity stated in the definition were also confirmed by the International Court of Justice ("ICJ") in the Gabcikovo-Nagymaros judgment.[16]

The plea of necessity, given its potential importance, did not escape the attention of the experts drafting the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (hereinafter "Tallinn Experts"), which devoted a separate rule 26 (Necessity) to it: "A State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."[17] Although the restatement of the rule in the Tallinn Manual is considerably more concise than in Article 25 of ARSIWA and does not contain all the conditions listed in Article 25, taking into account the commentary to rule 26 of the Tallinn Manual, it must be stated that the conditions within the scope of Article 25 of ARSIWA also form an integral part of this rule under the Tallinn Manual and "there is no substantial discrepancy" between these rules.[18]

A more detailed definition of the terms of the plea of necessity in the context of cyber operations will be discussed in the next part of this paper, but first it is necessary to define the differences between the plea

---

[11] ARSIWA 2001, Art. 25, para 2.

[12] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2.

[13] Hungary v. Slovakia (1997) International Court of Justice, Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia), para. 51 (hereinafter "Gabčíkovo-Nagymaros").

[14] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

[15] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 14.

[16] Gabcikovo-Nagymaros, para. 51.

[17] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

[18] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1624; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, pp. 137-141.

of necessity and retorsion, countermeasures and self-defence as possible alternatives to justify protective measures against a cyber operation in order to demonstrate comparative advantages and disadvantages of the plea of necessity.

1.2 ALTERNATIVE MEASURES OF RESPONES

The first, the least invasive, and arguably the least effective method of defence, is retorsion. Retorsion is defined as "retaliation for discourteous, or unkind, or unfair and inequitable acts by acts of the same or a similar kind".[19] It is therefore an act, which is unfriendly, but lawful. An example of the use of retorsion in response to a cyber operation is the European Union's action in 2020, when the EU imposed a travel ban and froze the assets of six individuals and three companies in connection with the Wanna Cry, Not Petya and Cloud Hopper operations.[20]

The second option that can be used to defend against a cyber operation is countermeasures. These are such non-forcible measures that an injured state adopts in response to an internationally wrongful act of another state which aim to compel that state to "cessation [of the internationally wrongful act] and to achieve reparation for the injury".[21] Unlike retorsion, which does not constitute a violation of international law, in the case of countermeasures the defending State commits an act which, although objectively fulfilling the elements of a wrongful act, the wrongfulness of the act is excluded precisely because it is a countermeasure within the meaning of Article 22 of ARSIWA. Thus, it is by reference to countermeasures that an interference with the sovereignty of another state can be justified, which gives the attacked state the possibility to use a wider range of cyber and other means to defend itself, including defensive cyber operation in the territory of responsible state (hack back).[22] However, invocation of countermeasures is also subject to several conditions.

---

[19] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press, p. 525 - 526.

[20] Council of the European Union. (2020) *EU Imposes the First Ever Sanctions against Cyber-Attacks.* [press release]. 30 July. Available from: https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ [Accessed 3 January 2022]; see also Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1173.

[21] ARSIWA 2001 with commentaries, Art. 22, p. 75, para. 1.

[22] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1179.

Countermeasures are only available if there is an internationally wrongful act committed by another state.[23] Thus, a prerequisite for the application of countermeasures is the attributability of the cyber operation to a state.[24] As noted above, the attributability of cyber operations is highly problematic, and countermeasures will therefore often not be available. Even if the cyber operation was attributed to a state, the countermeasures would still have to conform to other conditions: proportionality[25] and the prohibition of the threat or use of force.[26] Finally, countermeasures cannot be invoked against cyber operations launched by non-State actors, unless such conduct is attributable to the State.

The third alternative by which a state can respond to the most serious cyber operations that meet the characteristics of an "armed attack" under Article 51 of the UN Charter is self-defence.[27] the right to self-defence is an exception to the prohibition on the use and threat of force.[28] There are three issues associated with the right to self-defence in the context of cyber operations: the possibility of self-defence against non-State actors, attribution and the threshold of an armed attack.

The issue of the invocation of self-defence against armed attacks carried out by non-State actors is highly controversial. However, genuinely analyzing this issues would be out of scope of this paper. It will therefore only be pointed out that use of force against the territory of another State on the basis of cyber operations carried out by a non-State actor whose conduct is not attributable to that State is unlikely to be accepted by the international community as a valid justification of such act.[29]

---

[23] ARSIWA 2001 with commentaries, Art. 22, p. 75, para. 1; ARSIWA, Art. 2: "There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State."

[24] ARSIWA 2001 with commentaries, Art. 22, p. 75, para. 1.

[25] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1180.

[26] ARSIWA 2001, Art. 50(1)(a).

[27] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1619.

[28] Charter of the United Nations, 26 June 1945, article 2 (4).

[29] For indepth analysis see Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1177. See also United Nations Security Council, Resolution 1368 (2001) adopted on 12 September 2001 and United Nations Security Council, Resolution 1373 (2001) adopted on 28 September 2001; International Court of Justice. (2004) Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, para. 139 (hereinafter "Wall Advisory Opinion").

In relation to the issue of attribution, the problem is not so much the legal attribution itself, but rather the objective demonstration of the existence of a relationship between the cyber operation, the originator of the operation and the state. Thus, it is necessary to prove relationships at two levels. At the first level is the relationship between the cyber operation and its perpetrator, i.e. the actual finding of the originator of the operation (a specific device or person). At the second level, it is then a matter of demonstrating a relationship between the originator of the operation and the state that would satisfy the requirements of legal attribution.[30]

A third problematic aspect of the right to self-defence in the context of cyber operations is the determination of the threshold of an "armed attack". The ICJ has held that it is necessary to distinguish "the most grave forms of the use of force", which constitute an armed attack, from "other less grave forms", thus creating room for the use of force, which does not reach the threshold of an armed attack.[31] It can be concluded that the threshold of an armed attack in the cyber context remains unclear which severely limits the possibility of invocation of self-defence against cyber operations.[32]

A repertoire of legal instruments that states may have at their disposal in the event that they fall victim to a cyber operation has been presented. Each of them has its own drawback. Alongside these legal instruments stands the plea of necessity.

The plea of necessity has several advantages over the above options. In the first place, the plea of necessity justifies the violation of international law and thus allows, for example, a "hack back" operation to violate the sovereignty of another state. The fundamental advantage, then, is that the plea of necessity is available even if the cyber operation against which the victim state is defending itself is not attributable to another state, and it is thus available against non-state actors as well, distinguishing necessity from countermeasures and self-defense. In other words, a plea of necessity

---

[30] ARSIWA 2001 with commentaries, arts. 4-11.

[31] International Court of Justice. (1986) Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, para. 191.

[32] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1175; For a detailed analysis of approaches to "armed attack" in cyberspace see VALUCH, J and HAMUĽÁK, O. (2020) Use of Force in Cyberspace. *International and Comparative Law Review*, 20 (2), pp. 174-191.

can justify measures against a non-responsible State.[33] Plea of necessity can justify even "bleed-over effects" into third States.[34] Finally, unlike countermeasures, plea of necessity is available when harm is imminent, i.e. has not manifested yet.[35] Thus, it is clear that in the context of cyber operations, where the actions of non-State actors are widespread and attribution is often not possible, the plea of necessity is an instrument that can be very attractive for States threatened by cyber operations.[36] However, the plea of necessity is also inherently associated with a high risk of abuse, and therefore this legal instrument is limited by a number of conditions, to analysis of which is devoted the next section of this paper.

2. PRECONDITIONS AND LIMITATIONS OF THE PLEA OF NECESSITY

The main objective of international law is "to maintain peace and security through a rules-based system"[37] and the creation of the United Nations was motivated primarily by the objective "to maintain international peace and security".[38] the plea of necessity, while it can be a very effective tool in countering cyber operations, also carries the risk of abuse and escalation, and thus inherently threatens these goals of the international community.[39] It is therefore logical and correct that it is an exceptional measure with a high threshold, as already mentioned above, and that the use of this institute is limited by a number of strict conditions that must be insisted upon. We will therefore now turn to the interpretation of these conditions in the context of cyber operations.

---

[33] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 137.

[34] Ibid.

[35] Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. *The Cyber Defense Review*, 3 (2), p. 96.

[36] As Germany has also expressed in its official position on the application of international law in cyberspace, the plea of necessity is available "even in certain situations in which the prerequisites for countermeasures or self-defence are not met". The Federal Government Of Germany. (2021) *On the Application of International Law in Cyberspace*. [online] p. 14-15. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 4 January 2022].

[37] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1173.

[38] Charter of the United Nations, 26 June 1945, article 1(1).

[39] ARSIWA 2001 with commentaries, Art. 25, p. 80, para. 2; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1619.

2.1 PRECONDITIONS AND LIMITATIONS UNDER ART. 25 ARSIWA

2.1.1 ESSENTIAL INTEREST

A State can justify a measure on the basis of plea of necessity only if its "essential interest" is at stake.[40] the ILC Commentary to ARSIWA does not provide a definition of this term, but does provide that "[t]he extent to which a given interest is 'essential' depends on all circumstances, and cannot be prejudged".[41] Essential interest then undoubtedly cannot be limited to "solely a matter of the 'existence' of the State".[42] According to Tallinn Experts, it is true that "the determination of whether an interest is essential is always contextual".[43] A broader range of interests can be included among the essential interests. According to case law, these interests include protection of environment,[44] issues connected to financial obligations,[45] and protection of persons from terrorist attacks.[46] However, this list is by no means exhaustive and reflects only issues that have already been considered before international tribunals. Lotrionte includes among the essential interests "ecological equilibrium, economy, public health, safety, and maintenance of food supply for the population".[47] Schaller points out that essential interests may be interests related to "territorial integrity, political independence, and constitutional order of a State, the maintenance of public security, and the maintenance of the natural environment".[48]

If we focus on the state practice, we find that Germany includes under the concept of essential interest "certain critical infrastructures" and "protection of its citizens against serious physical harm" and

---

40 ARSIWA 2001, article 25(1)(a).

41 ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15.

42 International Law Commission. (1980) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two, p. 49, para. 32 (hereinafter "ARSIWA 1980 with commentaries").

43 Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge: Cambridge University Press, p. 135.

44 Gabčíkovo-Nagymaros, para. 53.

45 Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 208.

46 Lahmann derives the protection of persons from terrorist attacks as an essential interest from the advisory opinion on the Wall. See op. cit., p. 208, note 33.

47 Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. The *Cyber Defense Review*, 3 (2), p. 97.

48 Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1633.

the Netherlands conceives of essential interests more broadly as "services such as the electricity grid, water supply and the banking system".[49]

It is thus clear from the case law, academic literature and state practice listed above that a wide range of different interests can be subsumed under essential interests and, in essence, this is a relatively flexible condition, the fulfilment of which need not pose a major problem for States when invoking the plea of necessity.

Furthermore, the above positions of Germany and the Netherlands imply a considerable overlap between the concept of 'essential interest' and the concept of 'critical infrastructure', so we will look at this relationship in more detail.

The term "critical infrastructure" has no clear definition and different countries classify different technologies and systems under it.[50] However, a refinement of this concept is not necessary to define the relationship between "essential interests" and "critical infrastructure". According to Tallinn Experts, the classification of an infrastructure as critical is "suggestive" but not "determinative" in relation to determining whether it is an essential interest.[51] This means that not all critical infrastructure is essential interest, and at the same time infrastructure that is not designated as critical may be essential interest. The conclusion that not all critical infrastructure is classifiable as essential interest is also supported by the German national position on the plea of necessity cited above.[52]

If a cyber operation is carried out against the critical infrastructure of a State, then the decision whether the essential interest of that State has been interfered with has to be "objective and contextual in the sense of reasonableness in the circumstances".[53] Schmitt gives a pertinent example in which the subject of a cyber operation is healthcare cyber infrastructure, and in which he demonstrates the element of contextuality. Schmitt explains

---

[49] The Federal Government Of Germany. (2021) op. cit.; Government Of the Kingdom Of the Netherlands. *Appendix: International law in cyberspace*. [online] pp. 7-8. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 4 January 2022].

[50] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1632; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 135.

[51] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, pp. 135-136.

[52] Use of the phrase "certain critical infrastructure".

that in a case where a cyber operation disrupts a doctor's appointment system, the threshold of the essential interest of a State will not be crossed, but in a situation where a cyber operation "directed at blood banks during a natural disaster with ensuing significant loss of life" occurs, the threshold of essentiality will be crossed.[54] Similarly, a cyber operation aimed at disrupting the distribution of a vaccine against an infectious disease could be assessed. It will make a difference whether it is the distribution of a vaccine against a common seasonal flu or the distribution of a vaccine against covid-19 disease at the height of a pandemic wave during which hospitals are overcrowded. In the former case, the essential interest of a State is unlikely to be affected; in the latter, it probably is.

2.1.2 GRAVE AND IMMINENT PERIL

Another prerequisite to acting in the plea of necessity is that the essential interest is threatened by "grave and imminent peril".[55] the ILC has stated that "[t]he peril has to be objectively established and not merely apprehended as possible".[56] This idea was elaborated by the ICJ when it stated that peril "has to be duly established at the relevant point in time".[57]

Schaller defines "peril" as "a situation in which harm is likely to occur if no preventive action is taken".[58] While the ILC does not further define gravity, the Tallinn Experts agreed that in order for a "peril" to be considered "grave", such a threat must be particularly serious, disrupting an essential interest "in a fundamental way, such as destroying the interest

---

[53] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1185; Conversely, Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press on p. 209 does not consider the contextual nature and considers any operation that "partially or entirely disrupts" critical infrastructure as a grave peril.

[54] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 252; For another example of contextual analysis of essential interest see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1184.

[55] ARSIWA 2001, Article 25(1)(a).

[56] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15; Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale. p. 38.

[57] Gabčíkovo-Nagymaros, para. 54.

[58] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1633.

or rendering it largely dysfunctional".[59] However, the risk of causing material damage or injury is not a prerequisite for grave peril.[60] Germany considers "large-scale functional impairments" to be grave peril and, according to the Netherlands, the gravity must be assessed "on a case-by-case basis", while mere "impediment or inconvenience" cannot be considered grave peril.[61] In terms of severity, the plea of necessity does not require that the threatened consequences reach the level of an armed attack, which is also stated by France in in its national strategy.[62] It can be generalized that for the peril to be grave, the potential harm has to be objectively substantial. Following the above example of the attack on healthcare cyber infrastructure, it will certainly not be possible to consider as a grave peril merely making a hospital's website inaccessible to patients (equals to inconvenience), but disconnecting a hospital from its power supply with consequent damage to the health of patients dependent on the medical equipment will qualify as such.

The second qualifying criterion of peril is imminence. The inclusion of this characteristic in Art. 25 ARSIWA implies that the prerequisite for acting in plea of necessity is not the occurrence of damage, but it is possible to act anticipatorily.[63] the ILC has stated that "peril has to be imminent in the sence of proximity."[64] However, this does not mean that the imminence of the peril shall be considered only from the point of view of temporary element.[65] To the contrary, the ICJ held that "'peril' appearing in the long term might be held to be 'imminent' as soon as it is established, at the relevant point in time, that the realization of that peril, however far

---

[59] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University PressSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., p. 136.

[60] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 136; the Federal Government Of Germany. (2021) op. cit.; Government Of the Kingdom Of the Netherlands. op. cit., pp. 7-8.

[61] Ibid.

[62] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1188; The Federal Government Of Germany. (2021) op. cit.; Ministry Of Defence Of France. (2019) *International Law Applied to Operations in Cyberspace.* [online], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 5 January 2022].

[63] SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2), p. 251.

[64] ARSIWA with commentaries, Art. 25, p. 83, para. 15.

off it might be, is not thereby any less certain and inevitable".[66] At the same time, however, it should be borne in mind that another condition of the plea of necessity is that the action implemented (e.g. hack-back) must be the only way to protect the essential interest (see below). The greater the time lag between the discovery of the existence of the threat and its implementation, the more alternatives will generally be available to the injured state. This is also why the Tallinn Experts agreed that imminence in the context of plea of necessity has to be considered through the last "window of opportunity" standard applied in anticipatory self-defence.[67]

The Tallinn Manual 2.0 provides a number of examples of cyber operations for which the conditions of the plea of necessity can be considered satisfied. These include "a cyber operation that would debilitate the State's banking system, cause a dramatic loss of confidence in its stock market, ground flights nation-wide, halt all rail traffic, stop national pension and other social benefits, alter national health records in a manner endangering the health of the population, cause a major environmental disaster, shut down a large electrical grid, seriously disrupt the national food distribution network, or shut down the integrated air defence system".[68]

2.1.3 ONLY MEAN

It is clearly stipulated in the art. 25 of ARSIWA, that the plea of necessity is available only if there is no other way "to safeguard that [essential] interest", notwithstanding that possible alternative solutions are "more costly or less convenient".[69] Such alternatives may be purely technical solutions (e.g.

[65] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University PressSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., p. 138.

[66] Gabcikovo-Nagymaros, para. 54.

[67] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 139; see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1190 and Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1636.

[68] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 136.

[69] ARSIWA 2001 with commentaries, Art. 25(1)(a), p. 83, para. 15; see also Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1192;

moving operations from the damaged infrastructure to other available infrastructure),[70] the use of diplomatic procedures (see retorsion above), solutions through international organizations (e.g. referring the matter to the UN Security Council)[71] or other procedures, such as those listed in the Cyber Toolbox of the European Union.[72]

It is the "only mean available" condition that most often prevents the invocation of the plea of necessity.[73] Indeed, this was also the case in the repeatedly cited ICJ decision in Gabcikovo-Nagymaros, where the ICJ found that the "only means" condition was not met.[74] the ICJ reached the same conclusion in Wall Advisory Opinion.[75] Also, in the SolarWinds Operation case in 2020, the United States did not have the option of acting directly against Russia by reference to necessity, as other options were available (e. g. defensive cyber measures on the territory of the USA such as "sinkholing" the command and control domain of the malware).[76]

The importance of this condition is also evidenced by the fact that four of the six national positions mentioning the plea of necessity explicitly or

---

[70] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 139.

[71] ARSIWA 2001 with commentaries, Art. 25, p. 83, para. 15; Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 141.

[72] Council Of the European Union. (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* [online]. 10474/17, pp. 3-5. Available from: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf [Accessed 5 January 2022]; see also Schweighofer, E., Brunner, I. and Zanol, J. (2020) Malicious Cyber Operations, "Hackbacks" and International Law: an Austrian Example As a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 14 (2), p. 252.

[73] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 216.

[74] Gabčíkovo-Nagymaros, para. 55.

[75] Wall Advisory Opinion, para. 140.

[76] Schmitt, M. (2020) *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law.* [online] New York: Just Security. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [Accessed 5 January 2022].

implicitly (by reference to the terms of Article 25 of ARSIWA) mention this condition. These are Japan,[77] the Netherlands,[78] Norway[79] and Switzerland.[80]

2.1.4 IMPAIRMENT OF OTHER INTERESTS

Another condition limiting the availability of the plea of necessity is the prohibition of serious breach of the essential interest of another State or "the international community as a whole".[81] A prerequisite for the plea of necessity measure is not the attributability of the cyber operation to the State on whose territory the measure is to be carried out. Thus, it will often be a situation where the State of origin of the threat has no connection to the threat (for example, it is a cyber operation by an independent non-State actor). Therefore, unlike countermeasures and self-defence, the essential interest of that State must also be taken into account.[82] This idea is well captured by Schmitt when he stated that "states are precluded from addressing necessity situations if doing so would place any other state in comparable peril".[83] the practical implication of this plea of necessity concept is that a victim State whose essential interest is in a "grave an imminent peril", even if that essential interest "is far more significant" than the essential interest of another State that might be threatened by a possible response, cannot implement any defensive action on the basis of a plea of necessity that might threaten that less important essential interest of another State.[84] However, a different interpretation of Article

---

[77] Ministry Of Foreign Affairs Of Japan. (2021) *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* [online], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf [Accessed 5 January 2022].

[78] Government Of the Kingdom Of the Netherlands. op. cit., p. 7-8.

[79] United Nations. (2021) *Official compendium of voluntary national contributions.* [online]. Doc. A/76/136, 13 July 2021, p. 73. Available from: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf [Accessed 7 January 2022].

[80] Federal Department Of Foreign Affairs Of Switzerland. (2021) *Switzerland's position paper on the application of international law in cyberspace.* [online], p. 7. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 5 January 2022].

[81] ARSIWA 2021 with commentaries, Art. 15(1)(b).

[82] Countermeasures and self-defence have their own limits, of course, which must be respected in their application, but these are very different from the plea of necessity.

[83] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2)., p. 253;

[84] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Arimatsu, L. And SchmittSchmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press., M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1193.

25(1)(b) of ARSIWA is also strongly represented in the scholarly debate, according to which the balancing of essential interests on both sides is key and the plea of necessity is available in situations where the interest protected by virtue of its invocation is of a substantially higher value than the interest that may be impaired by the operation.[85]

2.1.5 EXCLUSION OF INVOKING NECESSITY

Invocation of the plea of necessity is explicitly ruled out in certain situations. It is the exclusion of the plea of necessity by another rule of international law and the situation where the State has contributed to the creation of the grave and imminent peril by its own conduct. [86]

In the first case, it is a situation where the use of necessity is excluded by a treaty (e.g. humanitarian conventions regulating ius in bellum) or these treaties containing their own plea of necessity regime which applies as lex specialis to the customary plea of necessity.[87] Necessity is not a peremptory norm of international law, and there is therefore nothing to prevent a contractual departure from the customary rule between the parties. The State is then obliged to respect this obligation and follow the special regime. Otherwise, it runs the risk of committing an internationally wrongful act by breaching an obligation arising from a treaty.

Invocation of the plea of necessity is also precluded in case the victim state has contributed to the peril by its own action or omission. The basic premise for assessing the contribution of a State is that any contribution is not sufficient, but it must be a contribution "sufficiently substantial and not merely incidental or peripheral".[88] One can agree with the Tallinn Experts' conclusion that a State's failure to protect its own cyberinfrastructure is not a sufficiently substantial contribution to preclude the applicability of the plea of necessity.[89] However, Lahnemman's conclusion that states are bound by a duty of due diligence to maintain up-to-date security of their own cyberinfrastructure, and thus if a grave and imminent peril arises

---

[85] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 221.

[86] ARSIWA 2001 with commentaries, Art. 25(2).

[87] ARSIWA 2001 with commentaries, Art. 25, p. 84, para. 19; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 225.

[88] ARSIWA 2021 wtih commentaries, Art. 25, p. 84, para. 20.

[89] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 140.

in connection with inadequate security of cyberinfrastructure, the State does not have the ability to apply the plea of necessity, seems questionable.[90] His conclusion does not adequately reflect the realities of cyberspace. First, it should be emphasized that malicious actors are always a step ahead of the victim and even the highest level of cyber security does not guarantee perfect protection. Secondly, the scale of cyber infrastructure in use in the public and private sectors and the limited capacity of a state to effectively ensure and enforce that the cyber security of these technologies is always up-to-date must also be taken into account. To accept such a strict interpretation of the plea of necessity conditions presented by Lahnemman would mean virtually eliminating the plea of necessity as a justification for measures taken in the context of cyber operations and it should therefore be refused.

2.2 LIMITATION OF PLEA OF NECESSITY NOT MENTIONED IN ART. 25 OF ARSIWA

States are limited in their right to invoke the plea of necessity by two other conditions that are not explicitly mentioned in Art. 25 of ARSIWA. These are the condition of the proportionality of the measure taken on the basis of the plea of necessity and the prohibition on use of the plea of necessity as a justification for a violation of a peremptory norm of international law under article 26 of ARSIWA.

First, let us look at the condition of proportionality. Measures taken under the plea of necessity are justified only to the extent that they are necessary "for preserving the essential interest threatened".[91] It is worth quoting the relevant part of the ILC's commentary on ARSIWA 1980: "Any conduct going beyond what is strictly necessary [...] will inevitably constitute a wrongful act per se, even if the plea of necessity is admissible as regards the remainder of the conduct. In particular, it is self-evident that once the peril has been averted by the adoption of conduct conflicting with the international obligation, the conduct will immediately become wrongful if persisted in, even though it has not been wrongful up to that point. "[92] Some authors have subsumed the proportionality aspect under the condition of "only means available", but such a subsumption is not

[90] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 228.

[91] ARSIWA 1980 with commentaries, Art. 33, pp. 49-50, para. 33.

[92] Ibid.

appropriate.[93] While the "only means" condition requires the selection of the most appropriate of the alternative measures, the assessment of proportionality should only be undertaken at the next step, once the means have been decided. Thus, if a plea of necessity hack back operation infringing on the sovereignty of another State is chosen as the appropriate (only) means to remove the threat, proportionality then requires an assessment of how to carry out the operation so as not to cause consequences more severe than necessary for preserving the essential interest. It follows that proportionality must be seen as a separate condition for the implementation of the plea of necessity. Similarly, a distinction is made between necessity (choice of means) and proportionality (proportionality to the aim pursued) as conditions of self-defence. [94]

Another condition limiting the repertoire of remedies available on the basis of the plea of necessity is found in Article 26 of ARSIWA, according to which "circustances precluding wrongfulness" including the plea of necessity cannot justify a violation of a peremptory norm of international law.[95] the ILC then explicitly mentions three rules of international law, the justification of the violation of which on the basis of plea of necessity is excluded, namely the prohibition of the use of force, the prohibition of genocide and the prohibition of killing of prisoners of war.[96] Which other rules of international law are peremptory norms is left to further interpretation by the ILC.[97] It is surprising that despite such a clearly articulated prohibition, the possibility of the use of force on the basis of the plea of necessity is still debated.[98] It is clear that the option of justifying the use of force on the basis of plea of necessity was not considered during the drafting of ARSIWA; on the contrary, it was ruled out. Furthermore, it can be argued that exceptions to the prohibition on the use of force should be approached restrictively, since the objective

---

[93] See Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press.Response Option to Hostile Cyber Operations. *International Law Studies*, 97 Response Option to Hostile Cyber Operations. *International Law Studies*, 97, p. 1192; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, p. 218.

[94] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press., pp. 549 - 550.

[95] ARSIWA 2001, Art. 26.

[96] ARSIWA 1980, Art. 33, p. 50, para. 37.

[97] Ibid.

of international law is to maintain international peace and security, and the creation of exceptions to the prohibition on the use of force is undoubtedly contrary to this objective (which is also the main objective of the UN).

Nevertheless, further development of the debate on the limits of the use of force in cyberspace is to be expected, because as long as there is a "grey zone" of the use of force, there is also the risk that what one state considers a non-forcible measure is a prohibited use of force for another state. Such a situation inherently contains the risk of unintended escalation and it is therefore in the interest of the international community to pay attention to this issue.

3. CONCLUSION

Cyber operations are a phenomenon that affects every State, and the question of legal measures to suppress them is a fundamental issue of international law. The plea of necessity is one of the unilateral remedies available. In contrast to countermeasures and self-defence, its application is not premised on the attributability of the cyber operation to the State, which is why this legal instrument has received increasing attention in scholarly debate and state practice.[99]

The core of this paper dealt with conditions of invocation of the plea of necessity. It was demonstrated that the first two conditions, i. e. (1) peril to the essential interest of a State which is (2) grave and imminent, do not pose a major challenge. Regarding these two conditions, it should only be pointed out that evaluation of the cyber operation has to be context dependent taking into account not just the nature of the target (e. g. hospital

[98] See e.g. Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press, p. 140; Vidmar, J. (2017) the Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111, pp. 301-306; Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97, pp. 1193-1194; Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press, pp.; Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1), p. 1621; Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale, p. 97.

[99] Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. The *Cyber Defense Review*, 3 (2), p. 96; Ohlin, J., D. and May, L. (2016) *Necessity in International Law*. 1st ed. New York: Oxford University Press. p. 39.

information system) but also the potential or actual consequences (a minor inconvenience compared to the death of patients).

On the contrary, the fact that the plea of necessity is only available if there are no other means applicable will prevent the invocation of this legal institute in most of scenarios. Generally, in the case of an unfriendly cyber operation victim States have at their disposal several protective measures (technical, diplomatic, and other) which do not require a breach of international law necessitating justification (in the form of the plea of necessity). If any of these measures can be used without invocation of the plea of necessity to effectively protect the essential interest against grave and imminent peril, they shall be used.

Another condition limiting the plea of necessity is the requirement not to breach the essential interest of another State including the State from whose territory the threat emanates. Two approaches were demonstrated. The first approach prohibits any interference with the essential interest of another State while the second approach uses proportionality as a criterion to distinguish between legal and illegal measures. The author of this paper is inclined to support the second approach which seems to more appropriately (fairly, if you wish) reflect the mutual rights and obligations among concerned States.

A victim State is also precluded from invoking the plea of necessity if it contributed to the peril by its own action or omission. In the paper, it was argued for the position that mere lack of up-to-date cyber security protection on the attacked computer system does not per se rule out the plea of necessity as such strict interpretation of the "contribution" condition would lead to the practical inapplicability of the necessity in the cyber context.

Probably the most important argument developed in this paper deals with the question of whether the plea of necessity can be used to justify the use of force. Even though authors arguing for legality of such approach can be found, in the present paper it was strongly argued for the opposite. Use of force is prohibited by a peremptory norm of international law. It was demonstrated with reference to the work of the ILC that the plea of necessity was never meant to justify a breach of peremptory norms and the prohibition of the use of force in particular. Only this conclusion is in line with the main objectives of the United Nations – to maintain

international peace and security. A different conclusion would unjustifiably raise the risk of escalation of the conflict.

Finally, in the analysis of the plea of necessity and prerequisites of its applicability in cyberspace attention was also paid to the state practice. So far, six states have officially announced their positions on the applicability of the plea of necessity in cyberspace and all of them agreed that, under strict conditions, the plea of necessity will be available. It can be expected that more states with a similar position will be forthcoming.

The aim of the article was to highlight some problematic aspects of the application of plea of necessity in the context of cyber operations. The plea of necessity can be an elegant solution to the problem of attributability of cyber operations to the state, which opens up the possibility of adopting justified protective measures. On the other hand, however, it is important to bear in mind the high risk of abuse, which has been repeatedly highlighted by the ILC and the expert community. To avoid such risk it is necessary to respect the condition of the plea of necessity summarized above and to continue the discussion on the interpretation of these conditions in the realm of cyber operations because the plea of necessity is here to stay.

LIST OF REFERENCES

[1] Arimatsu, L. And Schmitt, M. N. (2021) the Plea of Necessity: an Oft Overlooked Response Option to Hostile Cyber Operations. *International Law Studies*, 97.

[2] Bannelier, K. and Christakis, T. (2017) *Cyber-Attacks: Preventions-Reactions: the Role of States and Private Actors*. 1st ed. Paris: Les Cahiers de la Revue Défense Nationale.

[3] Center for Strategic & International Studies. (2022) *Significant cyber incidents.* [online] Washington, D. C.: CSIS. Available from: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [Accessed 3 January 2022].

[4] Council Of the European Union. (2017) *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")* [online]. 10474/17, pp. 3-5. Available from: https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf [Accessed 5 January 2022].

[5] Council of the European Union. (2020) *EU Imposes the First Ever Sanctions against Cyber-Attacks.* [press release]. 30 July. Available from:

https://www.consilium.europa.eu/en/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/ [Accessed 3 January 2022].

[6] Federal Department Of Foreign Affairs Of Switzerland. (2021) *Switzerland's position paper on the application of international law in cyberspace.* [online], p. 7. Available from: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf [Accessed 5 January 2022].

[7] Government Of the Kingdom Of the Netherlands. *Appendix: International law in cyberspace.* [online] pp. 7-8. Available from: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf [Accessed 4 January 2022].

[8] Grant, J. P. and Barker, C. J. (2009) *Parry & Grant encyclopaedic dictionary of international law*. 3rd ed. New York: Oxford University Press.

[9] *Charter of the United Nations,* 26 June 1945.

[10] International Court of Justice. (1986) Judgment of 27 June 1986, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*.

[11] International Court of Justice. (1997) Judgement of 25 September 1997, *Case Concerning the Gabčíkovo-Nagymaros Project (Hungary v. Slovakia).*

[12] International Court of Justice. (2004) Advisory Opinion of 9 July 2004, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory.*

[13] International Law Commission. (1980) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two.

[14] International Law Commission. (2001) *Yearbook of the International Law Commission: Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries*. vol. II, part two.

[15] Lahmann, H. (2020) *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution.* 1st ed. Cambridge: Cambridge University Press.

[16] Lotrionte, C. (2018) Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law. The *Cyber Defense Review*, 3 (2).

[17] Ministry Of Defence Of France. (2019) *International Law Applied to Operations in Cyberspace.* [online], p. 8. Available from: https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf [Accessed 5 January 2022].

[18] Ministry Of Foreign Affairs Of Japan. (2021) *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations.* [online], p. 5. Available from: https://www.mofa.go.jp/files/100200935.pdf [Accessed 5 January 2022].

[19] Ohlin, J., D. and May, L. (2016) *Necessity in International Law*. 1st ed. New York: Oxford University Press.

[20] Schaller, C. (2017) Beyond Self-Defense and Countermeasures: A Critical Assessment of the Tallinn Manual's Conception of Necessity. *Texas Law Review*. 95 (1).

[21] Schmitt, M. (2020) *Top Expert Backgrounder: Russia's SolarWinds Operation and International Law.* [online] New York: Just Security. Available from: https://www.justsecurity.org/73946/russias-solarwinds-operation-and-international-law/ [Accessed 5 January 2022].

[22] Schmitt, M. N. (2017) Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: an Analytical Vade Mecum. *Harvard National Security Journal*, 8 (2).

[23] Schmitt, M. N. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* 2nd ed. Cambridge: Cambridge University Press.

[24] Schweighofer, E., Brunner, I. and Zanol, J. (2020) Malicious Cyber Operations, "Hackbacks" and International Law: an Austrian Example As a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, 14 (2).

[25] The Federal Government Of Germany. (2021) *On the Application of International Law in Cyberspace.* [online] p. 14-15. Available from: https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf [Accessed 4 January 2022].

[26] United Nations Security Council, Resolution 1368 (2001) adopted on 12 September 2001.

[27] United Nations Security Council, Resolution 1373 (2001) adopted on 28 September 2001.

[28] United Nations. (2021) *Official compendium of voluntary national contributions*. [online]. Doc. A/76/136, 13 July 2021, p. 73. Available from: https://ccdcoe.org/uploads/2018/10/UN_-Official-compendium-of-national-contributions-on-how-international-law-applies-to-use-of-ICT-by-States_A-76-136-EN.pdf [Accessed 7 January 2022].

[29] United Nations. (2021) *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report.* [online]. Doc. A/AC.290/2021/CRP.2, 10 March 2021. Available from: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf [Accessed 7 January 2022].

[30] VALUCH, J and HAMUĽÁK, O. (2020) Use of Force in Cyberspace. *International and Comparative Law Review*, 20 (2).

[31] Vidmar, J. (2017) the Use of Force as a Plea of Necessity. *American Journal of International Law Unbound*, 111.

DOI 10.5817/MUJLT2022-2-5

AI-BASED DECISIONS AND DISAPPEARANCE OF LAW

by

YULIA RAZMETAEVA, NATALIA SATOKHINA*

Based on the philosophy of responsibility, the article examines, using the example of AI-based decisions, how the concept of responsibility changes under the influence of artificial intelligence, what unintended effect this conceptual shift has on our moral experience overall, and what implications it has for law. The problem of AI-based decisions illustrates well the general trend towards the transformation of the concept of responsibility, which consists in replacing personal responsibility with a system of collective insurance against risks. The disappearance of the capacity for responsibility from the structure of our experience, in turn, makes justice and law impossible.

KEY WORDS

Artificial Intelligence, AI-based Decisions, Responsibility, Experience of Law, Paul Ricoeur

1. INTRODUCTION

The last decade has seen an unprecedented growth of AI technologies, penetrating each and every aspect of our life from shopping to healthcare to driving your car. Each and every decision that people make seems to be prompted by AI, either indirectly (by influencing your choices) or directly (through decision-taking algorithms). According to Mireille Hildebrandt "*we are invited to learn to deal with an artificial world, 'peopled' by myriad of artificial agents that are becoming more and more smart and unpredictable*".[1] Whoever takes the decision may and will be held accountable for its consequences. If and when the decision is made by the algorithm,

* yulia.razmetaeva@gmail.com, nataliasatokhina@gmail.com, Department of Theory and Philosophy of Law, Yaroslav Mudryi National Law University, Kharkiv, Ukraine.

1 Hildebrandt, M. (2015) *Smart Technologies and The End(S) Of Law: Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar Publishing, p. ix.

the problem of accountability becomes acute and even irresolvable under the current law.

The issue of responsibility for AI-based decisions is widely discussed in the legal literature;[2] however, jurisprudence itself cannot offer a satisfactory solution here. It seems that in this case it is necessary to place the problem in a broader context. In particular, we propose to consider the issue of responsibility for AI decisions as part of a general trend towards the transformation of our understanding of responsibility and the corresponding moral experience, which consists in replacing personal responsibility with a system of collective insurance against risks. To do this, let us turn to the philosophy of responsibility, mainly the ideas of the French philosopher Paul Ricoeur.[3]

A more profound look at the phenomenon of responsibility enables us to single out its three components: the imputation of an action to its culprit, the retribution for the action and the compensation for the harm caused.[4] However, the example of AI-based decisions shows how the modern view on responsibility is reduced to a mere compensation for harm, excluding the imputation of an action to its culprit and retribution for the deed from the notion of responsibility. The latter is becoming more and more problematic as we can no longer determine with certainty: 1) who the culprit is and what exactly they should be blamed for, 2) what should be

[2] See: Brown, R. D. (2021) Property Ownership and the Legal Personhood of Artificial Intelligence. *Information & Communications Technology Law*, 30 (2), pp. 208-234. Available from: https://doi.org/10.1080/13600834.2020.1861714; Chen, J. and Burgess, P. (2019) The Boundaries of Legal Personhood: How Spontaneous Intelligence Can Problematise Differences between Humans, Artificial Intelligence, Companies and Animals. *Artificial Intelligence and Law*, 27, pp. 73–92. Available from: https://doi.org/10.1007/s10506-018-9229-x; Cofone, I. (2019) Algorithmic Discrimination Is an Information Problem. *Hastings Law Journal*, 70, pp. 1389-1444; Elish, M. (2019) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. *Engaging Science, Technology, and Society*, 5, pp. 40-60. Available from: https://doi.org/10.17351/ests2019.260; Floridi, L. (2021) The European Legislation on AI: A Brief Analysis of Its Philosophical Approach. *Philosophy & Technology*. Jun:1-8. Available from: https://doi.org/10.1007/s13347-021-00460-9; Hartmann, K. and Wenzelburger, G. (2021) Uncertainty, Risk and the Use of Algorithms in Policy Decisions: A Case Study on Criminal Justice in the USA. *Policy Sciences*, 54, pp. 269–287. Available from: https://doi.org/10.1007/s11077-020-09414-y; Gowder, P. (2018) Transformative Legal Technology and the Rule of Law. *University of Toronto Law Journa*l, 68, pp. 82-105. Available from: https://doi.org/10.3138/utlj.2017-0047; Jarota, M. (2021) Artificial Intelligence and Robotisation in the EU – Should We Change OHS Law? *Journal of Occupational Medicine and Toxicology*, 16, 18. Available from: https://doi.org/10.1186/s12995-021-00301-7; Sharkey, A. (2017) Can We Program or Train Robots to Be Good? *Ethics and Information Technology*. Available from: https://doi.org/10.1007/s10676-017-9425-5.

[3] For the philosophy of responsibility in general see for example: Jonas, H. (1985) *The Imperative of Responsibility: In Search of an Ethics for the Technological Age.* Chicago and London: The University of Chicago Press; Apel, K.-O. (1990) *Diskurs und Verantwortung: Das Problem des Übergangs zur postkonventionellen Moral*. Suhrkamp Verlag; Ricoeur, P. (2000) The *Just*. Chicago and London: The University of Chicago Press, pp. 11-35; Баумейстер, А. (2009) Imputatio. У: *Європейський словник філософій: Лексикон неперекладностей*. Т. 1. Київ: Дух і літера, сс. 485-497.

[4] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, pp. 11-35.

the adequate retribution for the act, and 3) what damage is compensable. Since responsibility is an integral part of law, the erosion of the concept of responsibility leads to a gradual disappearance of law from our life and its replacement by relationships of a completely different nature.

The edifice built upon these key elements is ruined when we deal with AI-based decisions as it becomes next to impossible to identify the culprit, since the rules applied to subjects of law are hardly applicable here. In the first place, even the most advanced AI has not yet been recognized as the subject of law. There have been some cautious attempts to do so or, at least, to leave room for interpretation that doesn't exclude subjectivity, for example, regarding copyright[5]. Such attempts are not an adequate solution to the problem since an algorithm cannot be regarded in terms of the conventional legal structures and cannot be seen as either of the traditional legal subjects: a natural person, a legal entity, a state, an international organization, etc. Besides, when investigating cases involving AI, identifying the culprit becomes next to impossible. In, say, a road accident caused by a self-driving car, is it the coding team behind the algorithm – which may consist of dozens of people, – the owners of the algorithm, or the company that produced the car – that should be held responsible? The deep neural network that offers an "automatic prediction of deterioration risks" in COVID-19 patients and prompts decisions for the clinicians[6] could probably not be considered a party – at least under the existing law – should the decision thus prompted lead to a fatality. An entirely different approach is needed, reconsidering our core beliefs as to what justice and responsibility are. This will make it possible to avoid the disappearance of law and prevent it from being substituted by a mere system of risks. Here, we attempt to showcase the possible outcomes of the present situation if left unchanged.

Based on the philosophical account of responsibility, we examine, using the example of AI-based decisions, how the concept of responsibility changes under the influence of AI, the unintended effect this conceptual shift has on our moral experience in general, and the consequences it has for law as an integral aspect of our existence. For this purpose, we are

[5] For example, in the case of a "literary, dramatic, musical or artistic work which is computer-generated, the author shall be taken to be the person by whom the arrangements necessary for the creation of the work are undertaken". See: Copyright, Designs and Patents Act of United Kingdom (1988). Available from: https://www.legislation.gov.uk/ukpga/1988/48 [Accessed 27 June 2021], 9(3).

[6] Shamout, F. E. et al. (2021) An Artificial Intelligence System for Predicting the Deterioration of COVID-19 Patients in the Emergency Department. npj Digit. Med. 4, 80. Available from: https://doi.org/10.1038/s41746-021-00453-0.

addressing the benefits and risks that stem from AI's decision making and the extent to which they can affect freedom, justice and the rule of law (part 2). We also observe the concept of responsibility changing in the modern world (part 3) and consider problems connected with the subject of responsibility (part 4). Besides, we look into the conventional understanding and limits of compensation for harm (part 5) and hypothesize about what consequences it has for law (part 6). Finally, using the EU law as an example, we investigate whether the existing legal framework is capable of preventing the loss of law without changing the conceptual approach (part 7).

2. ARTIFICIAL INTELLIGENCE IN DECISION MAKING

The spread of AI and AI-based decisions in all spheres of life is an inevitable and natural way of technological development, rather than a conscious value-based choice. It's a genie let out of the bottle, and chances are the genie will be ruling our reality. Harnessing the genie and making it serve us rather than enslave us (without us even being aware) is the purpose of today.

In taking decisions, algorithms appear to be able to far outdo humans. Algorithms are seemingly free from human error caused by emotions and/or physiology. It cannot be tired or angry. You would much rather have your X-ray interpreted by a robot that simply can't overlook that dark spot on your lung, than a human doctor, who has just had a family argument. AI is not subject to the influences stemming from human nature, and, as it is argued, that AI can be more objective in making decisions.[7]

AI is seemingly impartial. It is the ideal judge Hercules described by Ronald Dworkin as "*a lawyer of superhuman skill, learning, patience and acumen*",[8] which possesses limitless time resources and exhaustive knowledge. As such it can also help to impartially select those people who will make decisions in court or arbitration.[9] Besides, an algorithm can indirectly promote impartiality in decision-taking, by, in particular, substituting for a human being at certain stages of justice administrations

[7] Lepri, B. Oliver, N. and Pentland, A. (2021) Ethical Machines: The Human-centric Use of Artificial Intelligence. *iScience*, 24, 102249. Available from: https://doi.org/10.1016/j.isci.2021.102249.

[8] Dworkin, R. (1975) Hard Cases. *Harward Law Review*, 88 (6), p. 1083.

[9] Schwing, M. A. (2020) Don't Rage Against the Machine: Why AI May Be the Cure for the 'Moral Hazard' of Party Appointments. *Arbitration International*, 36(4), pp. 491-507. Available from: https://doi.org/10.1093/arbint/aiaa033.

and other legal processes. For instance, AI is supposed to be able to deal with privacy violations in international criminal procedure.[10]

AI is seemingly 100% accurate. Moreover, it is based on rules far simpler and more straightforward than the intricate knot of neural connections in the brain. When asked about the reasons of a decision a human being may not always be able to explain them. All too often, we make decision on a spur of the moment, guided by subconscious mechanisms we are unaware of. An algorithm's decisions can be traced back to their roots.

In particular, it is assumed that when leaders make decisions AI can increase accuracy of them due to its ever-growing computing power and real-time data usage.[11] In addition algorithmic decision-making promises to be highly efficient,[12] and economically beneficial due to improved quality of services at a lower cost.[13] Algorithms also able to help us make evidence-driven decisions.[14] As noted with the help of AI "intuitive decision-making can be replaced, or at least informed and supplemented by fact-based considerations".[15] Thus, the accuracy of AI in decision-making is strengthened by the circumstance that it is based on facts, evidence and data that are automatically processed, quickly and in large quantities.

Based on the above it appears that AI is the safest and the most reliable decision-making tool. We are increasingly tempted to entrust AI with a continuously growing range of decisions, given its capacity to quickly process huge amounts of data, make predictions with a much higher degree of probability, avoid cognitive biases and, ultimately, do it without interruption and without feeling tired. The result is that we increasingly tend to shift the burden of responsibility onto machines. Yet, is AI indeed what it seems to be?

More often than not AI turns out to be in fact partial and its decisions can increase bias. When compiled by a biased creator, the algorithms won't

[10] Segate, R. V. (2021) Cognitive Bias, Privacy Rights, and Digital Evidence in International Criminal Proceedings: Demystifying the Double-edged AI Revolution. *International Criminal Law Review*, 21(2), pp. 242-279. Available from: https://doi.org/10.1163/15718123-bja10048.

[11] Wang, Y. (2020) When Artificial Intelligence Meets Educational Leaders' Data-informed Decision-making: A Cautionary Tale. *Studies in Educational Evaluation*, 69, 100872. Available from: https://doi.org/10.1016/j.stueduc.2020.100872.

[12] Birhane, A. (2021) Algorithmic Injustice: A Relational Ethics Approach. *Patterns*, 2(2), 100205. Available from: https://doi.org/10.1016/j.patter.2021.100205.

[13] McGinnis, J. O. and Pearce, R. G. (2014) The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, 82(6), p. 3064.

[14] Aizenberg, E. and van den Hoven, J. (2020) Designing for Human Rights in AI. *Big Data and Society*, 7(2), pp. 1–14. Available from: https://doi.org/10.1177/2053951720949566.

[15] Groher, W. Rademacher, F.-W. and Csillaghy, A. (2019) Leveraging AI-based Decision Support for Opportunity Analysis. *Technology Innovation Management Review*, 9 (12), pp. 29-35. Available from: http://doi.org/10.22215/timreview/1289, p. 34.

be but biased as well. The data we feed AI may not sufficiently represent vulnerable groups or may bear the imprint of past discriminatory practices. This is well illustrated by the biases in AI designed for litigation, such as the racist AI's decisions based on court cases collected over the years, where the statistics of decisions made by white people were not in favor of blacks. The algorithm designed for rating a defendant's risk of committing crimes was prone to significant racial disparities: it is particularly likely to falsely flag black defendants as prospective criminals, while mislabelling white defendants as less likely offenders.[16] There are many more cases of algorithmic discrimination, which has been a growing concern over the past few years.[17]

In less morally loaded spheres, such as weather forecasting, natural disasters prediction, satellites trajectories planning, etc., the benefits of using AI are predominantly clear. However, in the same case of natural disasters AI doesn't seem to be reliable enough when it comes to resources allocation. All too often, resources are limited, and we are faced with moral dilemmas of who not to help for the sake of others. It appears that we can not and ought not to make algorithms responsible for ethical choices in situations that have a direct impact on people's lives, at least because such situations are emotionally sensitive and people seek to be helped by a compassionate human being rather than a "heartless machine".

Another example is legal processes. In complex and morally loaded cases with multiple controversial and contradictory circumstances, coupled with a complex balance of individual rights against legitimate interests, the AI will have to take into account too vast an array of considerations. So vast that it makes using AI hardly possible at all. Some cases may have no definitive resolution or a mathematically accurate answer whatsoever. Some cases are decided by an insignificant preponderance and there will be many disagreeing opinions and sharp discussions during and after the proceedings. By eliminating these "aftershocks" we leave no room for vital legal debates, which could identify and get rid of legislative gaps and contradictions. Examples may include decisions of the Grand Chamber

[16] Angwin, J. et al. (2016) Machine Bias. There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. *ProPublica*, 23th May. Available from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Accessed 24 October 2020].

[17] Williams, B. Brooks, C. and Shmargad, Y. (2018) How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications. *Journal of Information Policy*, 8, pp. 78-115; Cofone, I. (2019) Algorithmic Discrimination is an Information Problem. *Hastings Law Journal*, 70, pp. 1389-1444; Mazur, J. (2019) Automated Decision-making and the Precautionary Principle in EU Law. *Baltic Journal of European Studies*, 9 (4), pp. 3-18. Available from: https://doi.org/10.1515/bjes-2019-0035.

of the European Court of Human Rights in the case Vo v. France (2004),[18] in which it was debated whether or not an embryo has a right to life before it is born, or Evans v. United Kingdom (2007),[19] in which a woman's right to have genetically own children conflicted with the right of a man to withdraw his consent for the use of his genetic material. These cases also are examples of court disputes regarding sensitive issues, in which the general public have not reached a consensus, therefore it would be extremely inconsiderate to allow AI to make decisions of this kind. It is hardly sensible to empower algorithms with a possibility to deal with values.

Even without explicitly embedding value-based logic in AI it can and will implicitly contain certain ethical premises. An AI agent tends to function in accordance with the values of the customers or developers. When a team of developers is not sufficiently diverse, definite needs and problems specific to groups left non-represented can and will be overlooked. Focused on the logical and technical side, a developer cannot be fully aware of their subconscious premises and assumptions that can and will shape the resulting algorithm. This is clearly shown by many cases we have witnessed, such as elements of city design, crash test mannequins and drug tests prejudiced against women. There is no reason why algorithms won't adopt the same approach.

Another example of the complex case is the case of Bărbulescu v. Romania (2017)[20], where the court decided that there had been an infringement of privacy because the Romanian court was unable to determine the fair balance of the rights and interests of the parties, one of which, the employing company, was monitoring employers' correspondence in the workplace. This case stands out because the court's decision was changed to the opposite – but also because some judges actually changed their opinion. Is AI able to revise and change its decision?

One of the crucial parts of rule of law is the public being informed of the premises of decisions and the trust stemming from it. Precedent decisions often take into account the subtle nuances of the case as well as the validity and reasoning based on complex considerations, discussions and joint conclusions. People have access to the underlying argumentation no matter how complicated the case was. In contrast, AI-based decisions often do not contain explanations or detailed argumentation. This may

[18] Vo v. France, 53924/00, [2004] ECHR 326, (2005) 40 EHRR 12.

[19] Evans v United Kingdom, 6339/05, [2007] ECHR 264.

[20] Bărbulescu v. Romania, 61496/08, [2016] ECHR 61, [2017] ECHR 742, [2017] ECHR 754.

happen, for example, due to the very nature of some types of AI, such as neural networks, the reasons of whose actions often remain obscure to the developers themselves. Another reason for vagueness is that AI development and use is often the domain of companies reluctant to disclose the details of AI-based decisions. In addition, corporations are also often responsible for sacrificing the complexity and ethics of algorithms for the sake of functionality and a quick launch of a new product onto the market. If we actually do not have access to the internal mechanisms of the algorithm, some of the risks in using it can receive neither confirmation nor refutation.

Remarkably, AI is being used in decision support "in complex problems that involve uncertainty, large amounts of data, and are not deterministic".[21] While AI can be a boon for simple and repetitive tasks, not all uncertainty needs to be resolved. Certainty puts an end to discussion. Discussion, however, is part and parcel of law based on justice. Algorithmic and automatic decision making means less freedom. Without the freedom of action people don't develop ethical principles as part of their personality. If we aim to build a more and more mature society based on ever improving law, algorithmic decision-making will stand in the way.

All in all, AI may constrain freedom and undermine justice, in particular with regard to the responsibility-related issues they bring about. This, in turn, means problems for law as built upon justice, liberty and the recognition of human dignity. This is very close to the understanding of law as aimed at justice, in its antinomian understanding, which Mireille Hildebrandt advocated, when she defined law *"as aiming for justice, legal certainty and purposiveness"*.[22] Responsibility is a component of justice, which, in turn, is a component of law. The loss of responsibility causes significant damage to the two remaining components, to the point of their disappearance.

3. TRANSFORMATION OF THE IDEA OF RESPONSIBILITY

According to Paul Ricoeur, along with the capacities to speak, to act, and to talk about one's life, the capacity to take responsibility is the most important criterion of being a human and at the same time

[21] Phillips-Wren, G. and Jain, L. (2006) Artificial Intelligence for Decision Making. In B. Gabrys, R. J. Howlett and L. C. Jain (eds.) *Knowledge-Based Intelligent Information and Engineering Systems*. KES 2006. Lecture Notes in Computer Science, vol. 4252. Berlin and Heidelberg: Springer, pp. 531-536. Available from: https://doi.org/10.1007/11893004_69, p. 532.

[22] Hildebrandt, M. (2015) *Smart Technologies and The End(S) Of Law: Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar Publishing, p. 16.

the anthropological prerequisite of law. In its the most general form, the capacity for responsibility is understood as the ability to recognize that it's you who bears responsibility for your actions, as well as the ability the obligation to compensate the any damage caused by these actions and/or to undergo punishment for them. However, in the modern world, the relationships between the three elements of the concept of responsibility (imputation, compensation, retribution) are becoming more and more problematic, giving rise to a number of paradoxes like responsibility without fault, which in general leads that responsibility turning out to be *"a shattered concept"*.[23]

To restore integrity to this concept, Ricoeur proposes to return to Kantian double cosmological and ethical articulation of the term imputation, as the attribution of an action to an agent, and the moral qualification of that action. To this end, rather than referring to Kant's *Critique of Practical Reason* outlining the philosophy of law, one should address his *Critique of Pure Reason*, in particular the third "Cosmological Antinomy":

> *"Thesis: Causality, according to the laws of nature, is not the only causality operating to originate the phenomena of the world. A causality of freedom is also necessary to account fully for these phenomena.*
>
> *Antithesis: There is no such thing as freedom, but everything in the world happens solely according to the laws of nature".*[24]

The idea of imputability stems from the assumption of free spontaneity, whereby a series of appearances, which proceeds in accordance with laws of nature, begins with itself. In the *Critique of Practical Reason* this cosmological meaning of imputation is combined with the moral one: freedom constitutes the basis for the existence of the law, and the obligation to act in conformity with the law is combined with the duty to compensate for the damage or undergo punishment. It is this moral meaning of imputation that forms the basis of the modern legal understanding of responsibility, according to which the idea of retribution (for a fault) has displaced that of attribution (of an action to its agent). Thus,

[23] Ricoeur, P. (2000) *The Just.* Chicago and London: The University of Chicago Press, p. 19.

[24] Kant. I. (2003) *The Critiaue of Pure Reason.* Available from: https://www.gutenberg.org/files/4280/4280-h/4280-h.htm [Accessed 23 October 2020].

the cosmological component was gradually eliminated from the concept of responsibility.[25]

In reality, as Ricoeur notes, our actions are always associated with two types of causation, since, while performing a free action, we at the same time interfere in the course of events, which causes changes in the world.[26] However, the development of technology leads to free causality being gradually eliminated from our experience. This, in particular, is pointed out by Hannah Arendt when she speaks of a catastrophic deficit in the structure of our experience of thinking and acting.[27] The prospect of a radical transformation of our moral experience motivates as well the concerns of Jürgen Habermas about the rapidly developing biotechnologies which could lead to us no longer being able to understand ourselves as ethically free and responsible creatures.[28]

In jurisprudence, this deficit of action turns into deculpabilization of responsibility – its separation from the idea of fault, which is replaced by the concepts of solidarity, security and risk.[29] At the same time, fault is the central element of the concept of responsibility, which makes it possible both to attribute an action to its author and to undergo punishment for one's actions. Not accidentally that responsibility without fault seems to have appeared in jurisprudence quite late and until recently was rather an exceptional case. In turn, due to the exclusion of the element of fault both imputation and punishment are removed from the concept of responsibility. What remains is the third element alone, compensation for harm, which no longer presupposes identification of the actor, but only the one who bears certain risks, against which, however, you can always insure oneself.

> *"At the limit, however, we might ask whether there remains, at the end of an evolution where the idea of risk would have conquered the whole space of the law of responsibility, only a single obligation, that of insuring oneself against every risk!".*[30]

The result of these processes, according to Ricoeur, is a total loss of responsibility for any action. Being disconnected from the problematic

[25] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, pp. 13-19.
[26] Ricoeur, P. (2000) *The Just.* Chicago and London: The University of Chicago Press, p. 23.
[27] Arendt, H. (1998/1958) *The Human Condition*. Chicago and London: The University of Chicago Press, *pp.* 320-325.
[28] Habermas, J. (2003) *The Future of Human Nature*. Cambridge: Polity Press, pp. 16-74.
[29] *Ricoeur,* P. (2000) *The Just*. Chicago and London: The University of Chicago Press, p. 25.
[30] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, p. 28.

of decision-making, action finds itself placed under the sign of fatalism, which is the exact opposite of responsibility, because fate implicates no one, responsibility someone.[31]

Similarly, within the analysis of the history of this concept in the Western intellectual tradition, Andriy Baumeister points to the destruction of the idea of responsibility as going back from the Christian idea of human freedom and responsibility before God to the pre-Christian ideas of blind lot and fate.[32]

An example of such fatalism replacing responsibility is the increasingly widespread use of AI-based decisions in various fields, but especially in those that have always assumed personal responsibility: law, politics, medicine. The problem is that we don't understand who is the subject of fault and responsibility in the case of AI-based decisions, and who exactly should be blamed, what is the just retribution in this case, what kind of harm caused by AI-based decision is compensable. Is the notion of responsibility applicable here at all? Moreover, it could be said that such a destruction of the idea of responsibility leads to the loss of the very idea of law, at least the one that was formed in the Western tradition, that is, based on free will and responsibility.

4. THE SUBJECT OF RESPONSIBILITY

With this in mind it would be reasonable to consider the subject of responsibility in the light of AI-based decisions. Artificial intelligence could be seen as blurring the boundaries between human being and a machine. It is becoming increasingly complicated to distinguish between what the human being chose to do and what the machine designed to help them did. Machines are becoming parts of us: literally parts of our bodies, as cybernetic limbs, or almost literally parts of our brain, like computers, smartphones or driverless cars. In the past it used to be possible to separate an agent from the tool. It doesn't seem possible any longer. When your cyber eye malfunctions, is it you or the eye that is to blame for exceeding the limits of necessary defence? In many self-defence cases courts take into account the "*subjective perception of the attack*"[33] or the reasonable grounds

[31] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, p. 26.

[32] Баумейстер, А. (2009) Imputatio. У: *Європейський словник філософій: Лексикон неперекладностей*. Т. 1. Київ: Дух і літера, сс. 485-497.

[33] Novák, J. (2019) Assessment of the Impact of Acute Stress in Cases of Necessary Defense by Czech Courts. *Ido Movement for Culture. Journal of Martial Arts Anthropology*. Rzeszów: Idōkan Poland Association, 19 (1S), p. 90.

and beliefs of the one attacked. For instance, in the case *State v. Jones* (2016)[34] Whitlee Jones, having been attacked by her boyfriend, inflicted a mortal wound on him with a knife, believing that he would attack again. The court granted her immunity from prosecution, since she had been acting out of a reasonable belief of fear of death or grave bodily injury. In conventional cases like the above, we have an array of legal mechanisms to determine the measure of responsibility. For instance, it should be taken into account whether or not one mistook an innocent teenager for a criminal due to the thick fog, or whether or not a mental disorder played a role in your decision, etc. When a tool is inseparable from the agent it appears considerably harder, if at all possible, to determine the degree of responsibility.

If we are still looking for human subjects behind the algorithm, the circle of those responsible becomes too extended, since the circle of people involved in the creation, validation and implementation of AI is exceptionally wide. In addition, different parts of an algorithm could be assigned to different people, who may at some point change jobs; some corrections may be made to the code afterwards, making it increasingly difficult to trace the one responsible for a certain chunk of code. Apart from this, in the case of shared responsibility people tend to rely on everyone else. Each one of the team will only be shouldering a small fraction of responsibility. This behavioral effect is shown, for instance, in studies in two different social contexts: alone or in the presence of putative other third-party decision makers (full or diffused responsibility).[35]

While trying to determine the subjects of responsibility and the degree of guilt regarding AI-based decisions, we face numerous subjects involved and a disputable degree of their responsibility, which blurs the concept of responsibility as such. More often than not the user becomes the one carrying the entire burden of risks and responsibility. For instance, a user who submitted their credit card details through an application may sustaining financial losses or suffering from stress if the application doesn't function properly. Some of these losses are recoverable, but others are not, so these are additional risks that the end user assumes.

That said, can the algorithm itself acquire subjectivity, including a legal one? For the purpose of identifying the subject of responsibility in most

[34] State v. Jones, 416 S.C. 283, *786* S.E.2d 132 (S.C. 2016).

[35] Feng C. et al. (2016) Diffusion of Responsibility Attenuates Altruistic Punishment: A Functional Magnetic Resonance Imaging Effective Connectivity Study. *Human Brain Mapping*, 37, pp. 663–677.

cases guilt and intentions need to be taken into account. It probably isn't possible with AI. Even when dealing with strict liability under civil law, the key difference between the algorithm and another potentially dangerous "tool", such as a car or an attack dog, is the degree of autonomy. Some types of AI are at least capable of taking decisions and self-correcting, unlike dogs or cars. Potentially, it might become aware of itself, becoming very similar to a human being in that it can be regarded as a moral agent. If *"artificial agents extend the class of entities that can be involved in moral situations"*,[36] could they be seen as responsible? Will at least part of the moral responsibility lie with AI? How should we distribute responsibility among AI, its human developers, the customers, corporations, governments, etc.? If moral responsibility comes when agents are free to choose one action over another, what would be AI's preference? Will the algorithm ultimately acquire the ability to make ethical decisions based on what is ethically right or wrong? Will AI, in James H. Moor's terminology, become *"full ethical agents"* (being able to make ethical decisions, have free will, consciousness and intentionality)[37]?

Amanda Sharkey believes that *"given the gap between current robot abilities, and those required for full moral agency"*,[38] robots don't appear to ever be held morally accountable. When considering AI-based decisions, we can neither speak of AI's fault, nor regard it as a subject of moral and legal responsibility. It is perhaps worth concluding here that, when faced with unsolvable issues and not being able to identify the subject of responsibility, we will be forced to distribute the harm caused by AI-based decisions among all actors involved in the algorithm's development, sales, promotion and application. Such expansion of the circle of those held responsible is potentially endless and, by and large, leads to the fact that the concept of responsibility loses all meaning, at least legal, since the integral goal of legal responsibility – justice – is achievable only if responsibility is individualized, or at least the circle of responsible subjects is clearly limited. In turn, the elimination of fault and imputation from the concept of responsibility makes this goal unattainable.

Responsibility implies that we must establish what harm was caused and who must compensate for it. In legal cases where there is no subject

[36] Floridi, L. and Sanders, J. (2004) On the Morality of Artificial Agents. *Minds and Machines*, 14, pp. 349-379. Available from: https://doi.org/10.1023/B:MIND.0000035461.63578.9d.

[37] Moor, J. (2006) The Nature, Importance, and Difficulty of Machine Ethics. *IEEE Intelligent Systems*, 21 (4), pp. 18-21.

[38] Sharkey, A. (2017) Can We Program or Train Robots to Be Good? *Ethics and Information Technology*. Available from: https://doi.org/10.1007/s10676-017-9425-5.

of responsibility, there are at least compensation mechanisms (most often imposed on the state, sometimes on companies that produced the dangerous equipment or mistakenly released a defective batch of goods). In the case of AI, we have problems not only in establishing the subject of responsibility, but also in understanding and compensating for harm.

5. UNDERSTANDING HARM AND THE LIMITS OF ITS COMPENSATION

As far as harm is concerned the situation with autonomous vehicles appears to be the most illustrative. The well-known trolley problem that has fuelled philosophical debate for years has taken on a new dimension with the advent of fully AI-driven cars.

Philippa Foot outlined an ethical choice situation in which an uncontrollable trolley can either be turned onto the track where five people will be killed, or the track where one will be killed, discussing the "double effect doctrine", and the difference between direct and indirect intent, as well as a balance of good and evil.[39] Ever since then debates have been going on about the least harm and responsibility in a situation where it is impossible to avoid negative consequences. Judith Jarvis Thomson expanded on this problem by proposing to complicate it with the moral dilemma of the victim, where you have a choice not just between two tracks for the uncontrollable trolley, but between inaction and action – whether to push a large stranger standing on a bridge onto the path of the trolley where he will die stopping it.[40] Numerous variations of the dilemma have been springing up, the dilemma itself remaining rather theoretical – that is, until recently. Present day technological advances are pouring water onto the utilitarian's mill. Many of the AI technologies are based on utilitarian decision-making, and the deontological side of the discussion becomes eliminated.

AI makes us try to "solve" the trolley problem once and for all. When deciding on an action in a complicated road situation different human beings will be doing it in very different ways: based on intuition, based on spontaneous reactions, based on emotions or automatized skills. only a few will assess the potential harm. How will the algorithm be taking such

[39] Foot, P. (1967) The Problem of Abortion and the Doctrine of Double Effect. *Oxford Review*, 5, pp. 5-15.

[40] Thomson, J. (1985) The Trolley Problem. *Yale Law Journal*, 94, pp. 1395-1415. Available from: http://dx.doi.org/10.2307/796133.

decisions? What will be the underlying principle? There can be two possible logics behind this algorithm: the purely utilitarian one (potential harm assessment and/or assessment of the relative value of the lives of the people involved), or a random choice – based on a randomly generated number.

The moral agents mentioned above differ from other agents in that they have the responsibility to anticipate and avoid causing unjust harm. What understanding of unfair harm would AI use in a driverless car faced with the necessity of avoiding harm in a traffic accident? When it becomes part of our daily lives, should we be concerned when AI starts taking what we can call "ethical decisions"?

As some researchers suggest AI can minimize harm, while being ethical[41] and/or transparent.[42] However, what will be the definition of ethical? What is the definition of "just"? Algorithms are to be based on clearly defined principles while human decisions are taken based on an intricate mixture of intuitive and logical considerations. It is not unreasonable to assume that it's impossible, at least as of today, to create an algorithm that can take into account a wealth of complex ethical and logical considerations. Therefore, its solutions will have to be based on simple rules directed to minimizing harm. For instance, in a complicated road situation the algorithm will choose to swerve towards a sturdier car rather than the more fragile one, which will mean in essence punishing drivers of sturdier cars embedded in cars' algorithms. That might mean that a reckless driver of a Volkswagen Beetle is more likely to survive than a careful driver of a Range Rover, which is not the way we see justice today. Attempts to algorithmize the principle of minimal harm potentially give rise to at least two additional problems. People will have to be ranged in order to define sets of parameters for the algorithm. This is likely to be discriminatory as such sets will be limited, which means some people won't be taken into account. The other problem is that to make it possible for AI to assess people along those parameters a lot of data must be available and readable by it. That might entail, on the one hand, the necessity for people to share too many personal data, including age, chronic illnesses, disabilities and even pregnancy. On the other hand, this will mean having to install dozens of sensors and cameras, detecting the physical condition of a driver, their emotional state, etc., up to their sobriety.

[41] Geis, J. et al. (2019) Ethics of Artificial Intelligence in Radiology: Summary of the Joint European and North American Multisociety Statement. *Radiology*, 293(2), p. 439.

[42] Jobin, A. Ienca, M. and Vayena, E. (2019) The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*, 1, p. 391.

Both the philosophical and legal definitions of harm can be significantly different from how those engaged in machine learning understand harm. This might obscure the definition of liability. If new, complex and detailed laws and regulations are developed for such cases, then it is necessary for developers and customers (individuals, corporations and governments) to comply with them when introducing AI into operation. Such complex algorithms, however, probably won't be in demand, given the fact that, in essence, they are aimed at simplification. As has been shown above there is a limit to an algorithms' complexity. If an algorithm involves complex ethical considerations, will it have advantages over human decision-making as actually faster and more accurate, and will it work at all? In the case of self-teaching neural networks, the situation is complicated even further.

Bearing in mind the danger that AI will be built based on the utilitarian concept of minimizing harm, free from the complex ethical considerations that are nurtured in people throughout their lives, algorithmic decision-making should complement, rather than replace, human judgment. The problem is that such collaboration does not appear likely today. According to Paul Gowder, "*industry appears to rapidly working to computationally replicate the judgment previously carried out only by legally trained humans*".[43] Industry runs ahead of law and ethics while we are musing the issues of humanizing algorithms. Both in courts and on the road, we are getting closer to a truly autonomous AI that makes decisions but cannot be held responsible.

It is logical to conclude that the dehumanisation of AI-based mathematically justified decisions will lead to the dehumanisation of the idea of compensation for the harm done. Decisions prompted by the minimizing harm principle do not at all guarantee fairness as we, humans, see it today, while, at the same time, leading to the disappearance of the moral basis behind compensation in the form of the fault of the subject of choice. By and large, the harm caused by AI-based decisions is not subject to compensation within the framework of legal liability, and can only be covered by insurance payment.

6. DISAPPEARANCE OF LAW

The prevalence of technology, in particular, AI in decision-making leads to the situation when the actors multiply while the proportion of their responsibility is next to impossible to determine. The very concept

[43] Gowder, P. (2018) Transformative Legal Technology and the Rule of Law. *University of Toronto Law Journal*, 68, p. 82.

of responsibility becomes blurred. First and foremost, this can be seen as the difficulty identifying who is responsible in the sense of the author of harmful effects and, accordingly, as the difficulty individualizing responsibility (the problem of imputation). Secondly, the question arises: how far in space and time does the responsibility extend, and what becomes of the idea of reparation when there exists no relation of reciprocity between the authors of harmful effects and their victims?[44] The algorithm cannot be held responsible in any of the aspects of responsibility, and the circle of people involved in an algorithmic decision is potentially infinite. That said the circle of those affected by it is also potentially infinite, since the negative consequences of AI-based decisions can be delayed in time and affect many people. When this is the case, it is impossible to determine the circle of these people applying the criterion of the relationship between the actor and the affected person (the problem of compensation). Finally, the very concept of justice seems to be no longer relevant apart from the concept of free causality (the problem of retribution). Ricoeur summarizes these reasons for concern by calling on us to restore judgment and to preserve the idea of imputation, which is subject to attacks by solidarity and risk, again appealing to the Aristotelian virtue of *phronesis* – moral judgment conditioned by specific circumstances – which, according to Ricoeur, is a basis of the experience of law and justice.[45]

Notable in this regard is the conception of Lloyd L. Weinreb, who shows that the capacity for responsibility makes it possible to have rights. Accordingly, the erosion of the concept of responsibility makes our rights problematic. According to Weinreb, it is the idea of responsibility that underlies the difference between things and persons: things *cause* something to happen whereas people are *responsible* for what happens as a result of a decision.[46] Having the right means being responsible for our actions: having the right to do something, we also have the right not to do it, and thus, are responsible for our choices.[47] And in this sense, rights are not

[44] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, p. 30.

[45] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press, pp. 34f.

[46] Weinreb, Lloyd L. (2004) A Secular Theory of Natural Law. *Fordham Law Review*, 72 (6), pp. 2287-2300. Available from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3990&context=flr [Accessed 23 October 2020], p. 2291.

[47] Weinreb, Lloyd L. (2004) A Secular Theory of Natural Law. *Fordham Law Review*, 72 (6), pp. 2287-2300. Available from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3990&context=flr [Accessed 23 October 2020], p. 2295.

something that we should or should not have, but something that, along with responsibility, already exists as a *"moral fact"*.[48]

This leads us to the conclusion that the above described replacement of responsibility with insurance against risks and the subsequent gradual disappearance of the capacity to be the subject of imputation and retribution from our moral experience may entail the situation where the seemingly comfortable and secure world of AI-decisions turns out to be a world that no longer requires law.

7. AI-BASED DECISIONS UNDER THE EXISTING EU LAW

In order to see if there is any hope of avoiding the loss of law, with the existing legal solutions in the field of AI in mind, we will now make a brief analysis of EU law. We will focus on the European approach to AI regulation for two reasons that seem significant: (1) it is the most complete, consistent and all-encompassing to date, (2) it remains human rights centred.

The comprehensive legal framework is being discussed at the moment. It is long overdue as compulsory and fully harmonised technology, in order to avoid fragmentation of the European digital single market and promote innovation.[49] This has led to the emergence of promising proposal called the Artificial Intelligence Act,[50] which, among other things, grades AI systems by risk levels. According to Luciano Floridi, this regulation "*is a good starting point to ensure that the development of AI in the EU is ethically sound, legally acceptable, socially equitable, and environmentally sustainable*".[51] This is part of the overall tendency towards the creation of compulsory, comprehensive and extraterritorial framework. Other examples of the trend

[48] Weinreb, Lloyd L. (2004) A Secular Theory of Natural Law. *Fordham Law Review*, 72 (6), pp. 2287-2300. Available from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3990&context=flr [Accessed 23 October 2020], p. 2296.

[49] European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)). Available from: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html [Accessed 01 July 2021].

[50] EU Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM/2021/206 final. Available from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. [Accessed 21 June 2021].

[51] Floridi, L. (2021) The European Legislation on AI: A Brief Analysis of Its Philosophical Approach. *Philosophy & Technology*. Jun:1-8. Available from: https://doi.org/10.1007/s13347-021-00460-9.

are the Digital Markets Act,[52] the Digital Services Act[53] and Data Governance Act.[54]

That said, certain elements of regulatory basis for AI-based decisions exist already, although some of them take part in this regulation indirectly. In particular, norms regarding open data and data reuse,[55] are important to regulate algorithmic decision-making. It goes without saying that GDPR has a serious influence on AI application for two main reasons: it regulates handling the data that feed AI and influence its decisions, and, besides, it contains norms as to automated individual decision-making, including profiling.[56]

The extent to which the new regulatory suggestions will be coordinated with the existing acts is yet to be clarified. For instance, AIA defining an AI system as "*a software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with*".[57] Under the existing law, however, an AI system means "*a system that is either software-based or embedded in hardware devices, and that displays behaviour simulating intelligence by, inter alia, collecting and processing data, analysing and interpreting its environment, and by taking action, with some degree of autonomy, to achieve specific goals*".[58]

Alongside the problems of the new legal framework's comprehensiveness and the accordance of its elements, another issue

[52] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final. *Available* from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN [Accessed 27 June 2021].

[53] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN [Accessed 28 June 2021].

[54] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767 [Accessed 30 June 2021].

[55] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG [Accessed 19 June 2021].

[56] "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her", article 22, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 02 July 2021].

[57] EU Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM/2021/206 final. Available from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. [Accessed 21 June 2021].

appears essential: the ability of law to be anticipatory. According to Mirko Pečarič, "*the anticipative general legal rules are focused on the future*".[59] Given the overwhelming pace of technology development law is bound to be constantly lagging behind. To deal with this it is suggested that legislation should be adjusted to what is predicted to happen rather than be based on the "*classical binary legislation*".[60]

The aforementioned "digital" acts are supposed to form the carcass of the normative regulation of the emerging technologies. At the same time, their role appears to be restraining rather than determining. Apparently, we need to change the very approach. Law-makers need a broad range of consultations, primarily with philosophers, ethicists and IT technicians. All probable scenarios and all "ifs and buts" must be considered, including "digital" threats viewed in a broader context. Indeed, modern technologies may have a manipulative nature or influence,[61] and may influence social norms and expectations, frame cultural perceptions of accountability.[62] Algorithmization may disproportionately affect vulnerable groups, while also leading to the fact that complex social challenges are automated and packaged as mathematical problems,[63] and challenge us to ensure adequate levels of safety in work environments.[64]

As Kelly Blount rightly noted "*the effects of AI's use are not strictly limited to its immediate application*".[65] Algorithms may bear hidden risks. This is similar to the way social media significantly shape media landscape while

[58] European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice (2020/2013(INI)). Available from: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html [Accessed 17 June 2021].

[59] Pečarič, M. (2021) Lex Ex Machina: Reasons for Algorithmic Regulation. *Masaryk University Journal of Law and Technology*, 15(1), p. 111.

[60] Pečarič, M. (2021) Lex *Ex* Machina: Reasons for Algorithmic Regulation. *Masaryk University Journal of Law and Technology*, 15(1), p. 111.

[61] Susser, D. Roessler, B. and Nissenbaum, H. (2019) Technology, Autonomy, and Manipulation. *Internet Policy Review*, 8 (2). Available from: https://doi.org/10.14763/2019.2.1410; Klenk, M. (2020) Digital Well-being and Manipulation Online. In C. Burr and L. Floridi (eds.) *Ethics of Digital Well-Being: A Multidisciplinary Approach*. Dordrecht: Springer, pp. 81-100.

[62] Elish, M. (2019). Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. *Engaging Science, Technology, and Society*, 5, pp. 40-60. doi: https://doi.org/10.17351/ests2019.260.

[63] Birhane, A. (2021) Algorithmic Injustice: A Relational Ethics Approach. *Patterns*, 2(2), 100205. Available from: https://doi.org/10.1016/j.patter.2021.100205.

[64] Jarota, M. (2021) Artificial Intelligence and Robotisation in the EU - Should We Change OHS Law? *Journal of Occupational Medicine and Toxicology*, 16, 18. Available from: https://doi.org/10.1186/s12995-021-00301-7.

[65] Blount, K. (2021) Seeking Compatibility in Preventing Crime with Artificial Intelligence and Ensuring a Fair Trial. *Masaryk University Journal of Law and Technology*, 15(1), p. 45.

at the same time escaping editors' responsibility. Their normative role and impact on public debate had long remained concealed. Perhaps counter-intuitively, it is such merits of social networks as openness of opinions and civil society cooperation that made this problem non-obvious. These non obvious AI threats must undoubtedly be considered. Notwithstanding the rapidly developing legal framework, the approach to AI regulation must be modified in its core.

8. CONCLUSIONS

Further penetration of AI technologies into decision-making is inevitable. This will tell upon law in particular. There are obvious advantages of AI: it is efficient, its forecasts in less ethically loaded areas are accurate, it is relatively error-proof unlike human decisions, it contributes to overcoming inequality and systemic injustice. On the other hand, AI is associated with a number of risks: (1) the complexity of identifying the subject of responsibility and its limits, (2) difficulty determining the damage to be compensated, (3) the apparent impossibility of fair punishment.

As AI is literally merging with the human being and it is becoming increasingly complicated to identify the subject of responsibility. Being neither moral, nor legal a subject, AI, per se, can not be held responsible. When seeking a subject, we are faced with too broad a circle of them as there are too many actors involved in algorithmic decision-making. AI-dependent culture appears to emphasize the utilitarian mindset, which tells upon the understanding of harm and practically dehumanizes decision-making. Extra-complicated cases can arguably not be described by an algorithm, however complex. Any complexity has its limits while human nature manifestations have none. AI will cut off any deviations, thus, limiting the scope of the judiciary system and leading to injustice.

The described processes correlate with the general trend of transformation of the very concept of responsibility and the corresponding moral experience researched by Paul Ricoeur. This has to do with the replacement of personal responsibility with a system of collective insurance against risks and the disappearance of the capacity to be a subject of imputation and retribution from the structure of our experience. This, in turn, is making justice and law impossible. Ultimately, the world of AI-based decisions, in which we no longer need to make free and responsible decisions, no longer needs law.

Our dependence on algorithmic decision-making is growing at a much faster pace than the legislation can keep up with. There have been a large number of attempts to develop an effective legal framework to solve AI related problems. One of the most successful examples is the current EU legislation, as well as the proposals which are being actively discussed in EU. However, some threats remain hidden and are not even discussed.

We invented computers to help us think, to eliminate human errors, as the human being is imperfect. We take it for granted that intelligent machines are smarter than us, trusting algorithms far more than people. Surrounding ourselves with algorithms in each and every sphere of life we remain, however, unaware of the backward effect: we are starting to adopt the same style of thinking – the algorithmic one. We are making machines – machines are starting to make us. AI is designed to cope with human imperfection, but in doing so it eliminates doubt, removes the necessity of discussion, cuts out emotions and strips out the purely human things. Relying on algorithms heavily, we cannot but adopt this style of thinking as "better", internalizing it. At some point, we may unlearn to doubt and stop discussing for the sake of "rightness" and logic. At some point, we are bound to stop wanting fairness in the human understanding of the word – and substitute the mathematically ideal decision for a just decision. We will then become algorithmic fatalists.

This state of affairs is due to the very nature of the problem, which is not only and not so much legal as anthropological, and the solution of which requires combining the perspectives of jurisprudence, sciences and philosophy. The anthropological hope is that while we are still discussing this we still need human justice. We wouldn't want to reach a point at which we stop realizing that something is wrong, at which we stop striving for justice.

LIST OF REFERENCES

[1] Aizenberg E. and van den Hoven, J. (2020) Designing for Human Rights in AI. *Big Data and Society*, 7(2), pp. 1–14. Available from: https://doi.org/10.1177/2053951720949566.

[2] Angwin, J. et al. (2016) Machine Bias. There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks. *ProPublica*, 23th May. Available from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [Accessed 24 October 2020].

[3] Apel, K.-O. (1990) *Diskurs und Verantwortung: Das Problem des Übergangs zur postkonventionellen Moral*. Suhrkamp Verlag.

[4] Arendt, H. (1998/1958) *The Human Condition*. Chicago and London: The University of Chicago Press.

[5] Bărbulescu v. Romania, 61496/08, [2016] ECHR 61, [2017] ECHR 742, [2017] ECHR 754.

[6] Баумейстер, А. (2009) Imputatio. У: *Європейський словник філософій: Лексикон неперекладностей*. Т. 1. Київ: Дух і літера, сс. 485-497.

[7] Birhane, A. (2021) Algorithmic Injustice: A Relational Ethics Approach. *Patterns*, 2(2), 100205. Available from: https://doi.org/10.1016/j.patter.2021.100205.

[8] Blount, K. (2021) Seeking Compatibility in Preventing Crime with Artificial Intelligence and Ensuring a Fair Trial. *Masaryk University Journal of Law and Technology*, 15(1), pp. 25-51. Available from: https://doi.org/10.5817/MUJLT2021-1-2.

[9] Brown, R. D. (2021) Property Ownership and the Legal Personhood of Artificial Intelligence. *Information & Communications Technology Law*, 30(2), pp. 208-234. Available from: https://doi.org/10.1080/13600834.2020.1861714.

[10] Chen, J. and Burgess, P. (2019) The Boundaries of Legal Personhood: How Spontaneous Intelligence Can Problematise Differences between Humans, Artificial Intelligence, Companies and Animals. *Artificial Intelligence and Law*, 27, pp. 73–92. Available from: https://doi.org/10.1007/s10506-018-9229-x.

[11] Cofone, I. (2019) Algorithmic Discrimination is an Information Problem. *Hastings Law Journal*, 70, pp. 1389-1444.

[12] Copyright, Designs and Patents Act of United Kingdom (1988). Available from: https://www.legislation.gov.uk/ukpga/1988/48 [Accessed 27 June 2021].

[13] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information PE/28/2019/REV/1. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.172.01.0056.01.ENG [Accessed 19 June 2021].

[14] Dworkin, R. (1975) Hard Cases. *Harward Law Review*, 88 (6), pp. 1057-1109.

[15] Elish, M. (2019) Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction. *Engaging Science, Technology, and Society*, 5, pp. 40-60. Available from: https://doi.org/10.17351/ests2019.260.

[16] Evans v United Kingdom, 6339/05, [2007] ECHR 264.

[17] European Parliament resolution of 20 January 2021 on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice

(2020/2013(INI)). Available from: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0009_EN.html [Accessed 17 June 2021].

[18] European Parliament resolution of 20 October 2020 on intellectual property rights for the development of artificial intelligence technologies (2020/2015(INI)). Available from: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_EN.html [Accessed 01 July 2021].

[19] EU Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). COM/2021/206 final. Available from: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=COM:2021:206:FIN. [Accessed 21 June 2021].

[20] Geis, J. et al. (2019) Ethics of Artificial Intelligence in Radiology: Summary of the Joint European and North American Multisociety Statement. Radiology, 293(2), pp. 436-440. Available from: https://doi.org/10.1148/radiol.2019191586.

[21] Gowder, P. (2018) Transformative Legal Technology and the Rule of Law. *University of Toronto Law Journal*, 68, pp. 82-105. Available from: https://doi.org/10.3138/utlj.2017- 0047.

[22] Groher, W. Rademacher, F.-W. and Csillaghy, A. (2019) Leveraging AI-based Decision Support for Opportunity Analysis. *Technology Innovation Management Review*, 9 (12), pp. 29-35. Available from: http://doi.org/10.22215/timreview/1289.

[23] Feng C. et al. (2016) Diffusion of Responsibility Attenuates Altruistic Punishment: A Functional Magnetic Resonance Imaging Effective Connectivity Study. *Human Brain Mapping*, 37, pp. 663–677.

[24] Floridi, L. (2021) The European Legislation on AI: A Brief Analysis of Its Philosophical Approach. *Philosophy & Technology*, Jun:1-8. Available from: https://doi.org/10.1007/s13347-021-00460-9.

[25] Floridi, L. and Sanders, J. (2004) On the Morality of Artificial Agents. *Minds and Machines*, 14, pp. 349-379. Available from: https://doi.org/10.1023/B:MIND.0000035461.63578.9d.

[26] Foot, P. (1967) The Problem of Abortion and the Doctrine of Double Effect. *Oxford Review*, 5, pp. 5-15.

[27] Jarota, M. (2021) Artificial Intelligence and Robotisation in the EU – Should We Change OHS Law? *Journal of Occupational Medicine and Toxicology*, 16, 18. Available from: https://doi.org/10.1186/s12995-021-00301-7.

[28] Jobin, A. Ienca, M. and Vayena, E. (2019) The Global Landscape of AI Ethics Guidelines. *Nature Machine Intelligence*, 1, pp. 389–399. Available from: https://doi.org/10.1038/s42256-019-0088-2.

[29] Jonas, H. (1985) The Imperative of Responsibility: In *Search of an Ethics for the Technological Age*. Chicago and London: The University of Chicago Press.

[30] Habermas, J. (2003) *The Future of Human Nature*. Cambridge: Polity Press.

[31] Hartmann, K. and Wenzelburger, G. (2021) Uncertainty, Risk and the Use of Algorithms in Policy Decisions: A Case Study on Criminal Justice in the USA. *Policy Sciences*, 54, pp. 269–287. Available from: https://doi.org/10.1007/s11077-020-09414-y.

[32] Hildebrandt, M. (2015) *Smart Technologies and The End(S) Of Law: Novel Entanglements of Law and Technology*. Cheltenham: Edward Elgar Publishing.

[33] Kant, I. (2003) *The Critique of Pure Reason*. Available from: https://www.gutenberg.org/files/4280/4280-h/4280-h.htm [Accessed 23 October 2020].

[34] Klenk, M. (2020) Digital Well-being and Manipulation Online. In C. Burr and L. Floridi (eds.) *Ethics of Digital Well-Being: A Multidisciplinary Approach*. Dordrecht: Springer, pp. 81-100.

[35] Lepri, B. Oliver, N. and Pentland, A. (2021) Ethical Machines: The Human-centric Use of Artificial Intelligence. *iScience*, 24, 102249. Available from: https://doi.org/10.1016/j.isci.2021.102249.

[36] Mazur, J. (2019) Automated Decision-making and the Precautionary Principle in EU Law. *Baltic Journal of European Studies*, 9 (4), pp. 3-18. Available from: https://doi.org/10.1515/bjes-2019-0035.

[37] McGinnis, J. O. and Pearce, R. G. (2014) The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services. *Fordham Law Review*, 82(6), pp. 3041-3066. Available at: https://ir.lawnet.fordham.edu/flr/vol82/iss6/16.

[38] Moor, J. (2006) The Nature, Importance, and Difficulty of Machine Ethics. *IEEE Intelligent Systems*, 21 (4), pp. 18-21.

[39] Novák, J. (2019) Assessment of the Impact of Acute Stress in Cases of Necessary Defence by Czech Courts. *Ido Movement for Culture. Journal of Martial Arts Anthropology*. Rzeszów: Idōkan Poland Association, 19 (1S), pp. 89-91. Available from: https://doi.org/10.14589/ido.19.1S.13.

[40] Pečarič, M. (2021) Lex Ex Machina: Reasons for Algorithmic Regulation. *Masaryk University Journal of Law and Technology*, 15 (1), pp. 85-117. Available from: https://doi.org/10.5817/MUJLT2021-1-4.

[41] Phillips-Wren, G. and Jain, L. (2006) Artificial Intelligence for Decision Making. In B. Gabrys, R. J. Howlett and L. C. Jain (eds.) *Knowledge-Based Intelligent Information and*

Engineering Systems. KES 2006. Lecture Notes in Computer Science, vol. 4252. Berlin and Heidelberg: Springer, pp. 531-536. Available from: https://doi.org/10.1007/11893004_69.

[42] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN [Accessed 27 June 2021].

[43] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final. Available from: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM:2020:825:FIN [Accessed 28 June 2021].

[44] Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767 [Accessed 30 June 2021].

[45] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Available from: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 02 July 2021].

[46] Ricoeur, P. (2000) *The Just*. Chicago and London: The University of Chicago Press.

[47] Schwing, M. A. (2020) Don't Rage Against the Machine: Why AI May Be the Cure for the 'Moral Hazard' of Party Appointments. *Arbitration International*, 36 (4), pp. 491-507. Available from: https://doi.org/10.1093/arbint/aiaa033.

[48] Segate, R. V. (2021) Cognitive Bias, Privacy Rights, and Digital Evidence. *International Law Review*, 21(2), pp. 242-279. Available from: https://doi.org/10.1163/15718123-bja10048.

[49] Shamout, F. E. et al. (2021) An Artificial Intelligence System for Predicting the Deterioration of COVID-19 Patients in the Emergency Department. *npj Digit. Med*. 4, 80. Available from: https://doi.org/10.1038/s41746-021-00453-0.

[50] Sharkey, A. (2017) Can We Program or Train Robots to Be Good? *Ethics and Information Technology*. Available from: https://doi.org/10.1007/s10676-017-9425-5.

[51] State v. Jones, 416 S.C. 283, 786 S.E.2d 132 (S.C. 2016).

[52] Susser, D. Roessler, B. and Nissenbaum, H. (2019) Technology, Autonomy, and Manipulation. *Internet Policy Review*, 8 (2). Available from: https://doi.org/10.14763/2019.2.1410.

[53] Thomson, J. (1985) The Trolley Problem. *Yale Law Journal*, 94, pp. 1395-1415. Available from: http://dx.doi.org/10.2307/796133.

[54] Vo v. France, 53924/00, [2004] ECHR 326, (2005) 40 EHRR 12.

[55] Wang, Y. (2020) When Artificial Intelligence Meets Educational Leaders' Data-informed Decision-making: A Cautionary Tale. *Studies in Educational Evaluation*, 69, 100872. Available from: https://doi.org/10.1016/j.stueduc.2020.100872.

[56] Weinreb, Lloyd L. (2004) A Secular Theory of Natural Law. *Fordham Law Review*, 72 (6), pp. 2287-2300. Available from: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3990&context=flr [Accessed 23 October 2020].

[57] Williams, B. Brooks, C. and Shmargad, Y. (2018) How Algorithms Discriminate Based on Data They Lack: Challenges, Solutions, and Policy Implications. *Journal of Information Policy*, 8, pp. 78-115.

MUJLT Official Partner (Czech Republic)

ROWAN LEGAL, advokátní kancelář s.r.o.
www.rowanlegal.com/cz/

Cyberspace 2021 Partners

Vodafone Czech Republic
www.vodafone.cz

Wolters Kluwer
www.aspi.cz

Zákony pro lidi - AION CS
www.zakonyprolidi.cz

CODEXIS - ATLAS consulting
www.codexis.cz

Notes for Contributors

Focus and Scope

Masaryk University Journal of Law and Technology (ISSN on-line 1802-5951, ISSN printed 1802-5943) is a peer-reviewed academic journal which publishes original articles in the field of information and communication technology law. All submissions should deal with phenomena related to law in modern technologies (e.g. privacy and data protection, intellectual property, biotechnologies, cyber security and cyber warfare, energy law). We prefer submissions dealing with contemporary issues.

Structure of research articles

Each research article should contain a title, a name of the author, an e-mail, keywords, an abstract (max. 1 500 characters including spaces), a text (max. 45 000 characters including spaces and footnotes) and list of references.

Structure of comments

All comments should contain a title, a name of the author, an e-mail, keywords, a text (max. 18 000 characters) and a list of references.

Structure of book reviews

Each book review should contain a title of the book, a name of the author, an e-mail, a full citation, a text (max. 18 000 characters) and a list of references.

Structure of citations

Citations in accordance with AGPS Style Guide 5th ed. (Harvard standard), examples:

Book, one author: Dahl, R. (2004) *Charlie and the Chocolate Factory*. 6th ed. New York: Knopf.
Book, multiple authors: Daniels, K., Patterson, G. and Dunston, Y. (2014) *The Ultimate Student Teaching Guide.* 2nd ed. Los Angeles: SAGE Publications, pp.145-151.
Article: Battilana, J. and Casciaro, T. (2013) The Network Secrets of Great Change Agents. *Harvard Business Review*, 91(7) pp. 62-68.
Case: *Evans v. Governor of H. M. Prison Brockhill* (1985) [unreported] Court of Appeal (Civil Division), 19 June.
Citation Guide is available from: https://journals.muni.cz/public/journals/36/download/Citationguide.pdf

Formatting recommendations

Use of automatic styles, automatic text and bold characters should be omitted.
Use of any special forms of formatting, pictures, graphs, etc. should be consulted.
Only automatic footnotes should be used for notes, citations, etc.
Blank lines should be used only to divide chapters (not paragraphs).
First words of paragraphs should not be indented.
Chapters should be numbered in ordinary way – example: "5.2 Partial Conclusions".

Submissions

Further information available at
https://journals.muni.cz/mujlt/about

LIST OF ARTICLES