Ambrus, István*

Digitalisation and the Criminal Law

Digitalisation has been an increasingly dominant concept in our daily lives since around the turn of the millennium, and the pandemic of 2020–2021 will see the scale and volume of digital usage reach unprecedented levels. Multi-activity, previously almost unthinkable, has moved online. However, we now take it for granted that we give academic lectures, attend conferences or participate in litigation using our computers or smartphones and tablets. At its extraordinary meeting on 1–2 October 2020, the European Council stated that digitalisation will be one of the two main pillars of the EU's recovery from the Covid19 crisis and, as such, will play a key role in stimulating new forms of growth and strengthening the EU's resilience.[1] This finding also foreshadows that the role of digital tools will remain as strong after the pandemic, and that technologies such as artificial intelligence, algorithmic decision-making and blockchain could lead to further leaps forward.

Although the classical notion of digitalisation was essentially the transformation of ontological phenomena into a computer-readable form, typically written in binary numbers, the concept has now acquired a number of additional meanings. Thus, "digital" is now a generic term that can cover any interaction – financial, commercial, administrative, judicial, private, etc. – that takes place mostly on the Internet, in cyberspace.[2] According to Susanne Beck, digitalisation encompasses not only technological changes (in particular the emergence and continuous development of the Internet) but also the social processes that have taken place as a result. She sees the biggest catalyst for this, on the one hand, in the potential for almost unlimited data collection ("Big Data") and, on the other, in the deep learning method, whereby computer processing can lead to increasingly less predictable (indeterministic) results.[3]

All of this makes it clear that we are now in a true digital age, with citizens having mass access to digital tools, which means that even the most mundane activities

* Ambrus, István, Dr. habil., Habitilitated Associate Professor, Eötvös Loránd University, Faculty of Law, Department of Criminal Law.

1 https://www.consilium.europa.eu/hu/policies/a-digital-future-for-europe/ (Last accessed: 30 December 2021).

2 T. Kiss, A kibertér fogalma, in T. Kiss (ed.), *Kibervédelem a bűnügyi tudományokban,* (Dialóg Campus, Budapest, 2020) 9–12.

3 S. Beck, Die Diffusion strafrechtlicher Verantwortlichkeit durch Digitalisierung und Lernende Systeme, (2020) (2) *Zeitschrift für Internationale Strafrechtsdogmatik,* 41–50., 41.

DOI: 10.56749/annales.elteajk.2021.lx.14.215

are often carried out online.[4] More recently, the concept of digital identity has emerged, whereby one's constant presence online has made it possible to map people's daily lives to a previously unimaginable degree, making it almost possible to create a digital copy of oneself.[5] This process can be facilitated by the Internet of Things, which links all digital devices, accounts, codes, etc. belonging to the same person.

As far as the legal system is concerned, there is no doubt that it must always react to technological innovations, as it has done in the past, for example with the invention of electric power and the telephone. Today, however, digital development has accelerated to such an extent that it may entail almost constant monitoring and amendments to the relevant legislation. This is by no means limited to sectoral or detailed rules. The widespread use of phenomena such as artificial intelligence may also require a rethinking of the fundamental concepts of certain branches of law. This is no different in the case of criminal law, which is the sanctioning pillar of the entire legal system, where, although the adherence to dogmatic traditions is very strong, new technological solutions may even require a comprehensive revision. The present work is intended to help in this respect, since I believe that the observation that "criminal law in particular is lagging behind the changes of life' is well-founded. The legislator learns of the need for legislation from life experience, social expectations and the reactions of the legislator's administration but, even then, it takes a long time before legislation is enacted and put into practice. [...] These observations are particularly true for computers and cybercrime".[6]

This thesis is entitled Digitalisation and the Criminal Law. The simplistic title obviously requires some explanation. The term "criminal law" should be understood in the narrow sense of the term, which refers exclusively to substantive criminal law. The thesis therefore does not deal with criminal procedural law, which is also facing many challenges as a result of digitalisation, or with the law of the penitentiary system. It also does not go into detail on the relevant findings of the broader criminal sciences, such as (empirical) disciplines like criminology.[7] There is also no separate legal history or comparative law section, although, particularly in the chapters dealing with specific offences, I have done as much historical and external research as the subject requires.

The choice of topic, while rewarding for its high actuality, in fact entails a number of risks. First and foremost is the expected lack of temporality. Since the technologies under discussion are currently undergoing constant development and change, it is easy

[4] https://dictionary.cambridge.org/dictionary/english/digital-age (Last accessed: 30 December 2021).
[5] M. Oswald, Jordan's dilemma: Can large parties still be intimate? Redefining public, private and the misuse of the digital person, (2017) 26 (1) *Information & Communications Technology Law,* 6–31. https://doi.org/10.1080/13600834.2017.1269870. Also see A. M. Froomkin, The Death of Privacy? (2000) 52 (5) *Stanford Law Review,* 1461–1543. https://doi.org/10.2307/1229519
[6] V. Vadász, A számítógép demisztifikálása, (2010) 17 (2) *Ügyészek Lapja,* 13–21., 13.
[7] See J. Clough, *Principles of Cybercrime,* (Cambridge University Press, Cambridge, 2010) 8–10.

to see how some of the findings of the thesis could quickly become obsolete. For my part, I believe that this problem can at least partially be avoided by devoting a separate chapter to the emerging issues of criminal law doctrine, which, although they will be modified – and I will argue on several occasions that digitalisation will make it necessary to reinterpret them – should be changed more slowly and with much greater care than in the densely modified material of the special part of criminal law. On the other hand, a more rapid expiry of the 'statute of limitations' can be seen as a natural consequence of circumstances. Previously, millennia had passed between the appearance of two new technical achievements, such as the horse-drawn carriage and the motor car. However today, to take an example from the world of music, while today's early thirty-somethings, who listened to cassette tapes as children and switched to CDs in high school, were dominated by computer mp3s as university students, are now almost exclusively using streaming music providers. So, for the first decades of the 21st century, we are essentially living through a constant revolution of discovery. As the author of a recent national study puts it, "[t]his revolution, though based on technology, is not technological. In other words, it does not reform technology, but by using technology it can change our whole lives, perhaps even our centuries-old, millennia-old social arrangements".[8] This will necessarily entail at least partial obsolescence of the literature on the subject, even in the medium term. Even do, this is not to be feared; it is a natural part of progress.

Another problem is that the topic may seem too broad, as there is virtually no area of our lives that is not directly or indirectly affected by digitalisation. In view of this, it was not possible to aim for completeness, but instead to select from an almost infinite number of sub-topics, which could, of course, also entail the risk of arbitrariness in the selection of topics. I have sought to overcome this problem by providing a panoramic overview of the issues of relevance to criminal law in the field of digitisation. Thus, in addition to analysing the relevant provisions of the Criminal Code, I have selected other subjects which are at the centre of interest in both public discourse and legal studies. I have also endeavoured to meet the requirement of internal proportionality, but it is obviously not possible to write about completely new phenomena, the technology of which is still at a stage of considerable development, to the same extent as about instruments that are already established and have been the subject of judicial practice. In view of this, there is therefore no separate chapter on, for example, the aforementioned blockchain, which is likely to continue to dominate digital everyday life in the short term, or on smart contracts, which are not primarily of criminal law relevance.

The thesis is structured in four main chapters and two excursuses. The first two major chapters form the "general part" of the work: here, after presenting views on the

[8] Z. N. Sík, A blockchain filozófiája, avagy fennálló társadalmi rendek felülvizsgálatának kényszere, (2017) 10 (4) *Új Magyar Közigazgatás,* 37–56., 37.

concept of crime, I turn to the impact of digitalisation on certain dogmatic categories. I will outline the new scientific concept of the offence, the doctrine of quasi-open crime, and the reasons for the increased importance of preparation and inept attempts. As regards the new penal issues, I briefly touch upon the problems of the rules of cognitive punishment and the new measure most closely linked to digitalisation, namely the permanent inaccessibility of electronic data.

I should point out here that I have classified the sections which would have been covered by both the general and the special sections according to their primary nature and have dealt with them in the appropriate place in the thesis, for example, although there is a separate chapter on bank card offences, I have dealt with the issue of inappropriate attempts to commit these offences in the criminal law section.

The first part of the "special section" is more closely linked to the substantive law and analyses the most relevant offences in the context of digitisation in the light of the relevant literature and case law. The distinction between digital offences in the narrow and broad sense will be elaborated. In the former, I will discuss information system offences and the problem of ethical hacking on the one hand, and offences related to cash substitutes on the other, including cryptocurrencies. Third, I will look at the offences that can be committed in connection with data, including drones, which will be a sui generis offence in Hungary from 1 January 2021.

Digital crimes in the broader sense can include a myriad of offences, but it was necessary to highlight those with the greatest theoretical and practical relevance. In this context, I have analysed child pornography and harassment and, as a specific issue, the emergence of a new type of criminal offence against property in the commercial world. In a separate section, I discuss the offence of money laundering, which will also be fully reorganised from 1 January 2021, and then I turn to offences that can be committed on the internet and social media, such as incitement to hatred, threats of terrorist acts, threats of public danger, spreading of scandal, defamation and the related phenomenon of "fake news".

In the next major chapter on the new challenges of digitalisation, I will introduce artificial intelligence, with a particular focus on the impact of this technology on the conceptual elements of crime. Closely related, but due to its connection with traffic criminal law, the issue of self-driving vehicles will be presented in a separate chapter. A further dilemma in transport law is the legal status of new devices such as electronic scooters and the segway.

In a separate sub-chapter, I will deal with new types of sexual offences such as revenge pornography, upskirting, cyberflashing and deepfake, which can also be (partly) identified as a sexual offence.

As I have indicated, the work also includes two so-called excursuses – indirectly related to the main topic – one of which is an examination of the criminal law issues of the Covid19 epidemic, which will be inevitable in the light of the developments in 2020,

while at the same time, for the sake of completeness, covering not only the acts that can be committed in the digital space, but also the acts that can be committed in the context of virus infections in general. The second excursus contains my reflections on an otherwise essentially "offline" offence, the social perception of which has undergone a significant change as a result of digitalisation, and in particular of crimes posted on social networking sites, which is expected to lead to a change in the relevant legislation in the near future, namely the criminal offence of animal cruelty.

In this thesis, I have sought to carry out primarily a criminal law-dogmatic analysis by evaluating and contrasting the views expressed in the literature and in case law and in the legislative process. In many cases, I have assessed changing practice, the law in general, and made *de lege ferenda* suggestions for future legislation. In addition to exploring domestic sources, I have sought to draw primarily on the results of Anglo-Saxon and German legal literature, and have also made international surveys in a number of areas. In some chapters, where this seemed appropriate, I have also provided a partial summary and highlighted my specific, bulleted theses.

This research was supported by Eötvös Loránd University, Faculty of Law, and also the National Research, Development and Innovation Office through the Postdoctoral Excellence Programme PD_18 No. 128394 and by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office through the National Laboratory for Artificial Intelligence, for which I am grateful.