# Legal Tech in the Law Enforcement Agencies

*Maria Dymitruk*

## *1. Introduction*

The tasks of the law enforcement agencies are primarily concerned with crime prevention, maintaining public order and security as well as detecting and prosecuting offences through pre-trial investigations. Their activities are largely coercive, and they deal not only with the criminal offence and its perpetrators, but also with a wide range of cases in which it is not known whether a given act constitutes a criminal offence or who the actual perpetrator is, as well as cases in which the aim of the authorities' actions is not to detect a crime but to ensure that it is not committed (e.g. in securing the order of public demonstrations). In this way, the activities of the law enforcement authorities concern an indefinite circle of people, including citizens whose activity is in no way directed towards actions of a criminal nature.

The work performed by law enforcement agencies is significantly facilitated (and often improved) by technological development[1]. Of course, the intensification of the use of more and more advanced IT solutions is a double-edged weapon: on the one hand it provides law enforcement agencies with tools enabling faster, more efficient and more reliable detection of crime and prosecution of its perpetrators, and on the other hand it allows the use of highly developed IT solutions for criminal purposes. The issue of identifying the right technological response to 'innovative crime' by law enforcement agencies remains therefore of utmost importance. It should also be noted that technological tools can be used by the law enforcement agencies to detect traditionally committed criminal acts. A good example of such application of the technology is a system recognizing a potential thief face in a crowd, based on a facial recognition system, i.e. a system for

1 This thesis is valid not only in the 21st century. The influence of technological development on the activities of police authorities is a constant phenomenon - see Mathieu Deflem and Stephen Chicoine, 'History of Technology in Policing' in Gerben Bruinsma and David Weisburd (eds), *Encyclopedia of Criminology and Criminal Justice* (Springer 2017) 2269 – 2277.

automatic identification of individuals based on individual facial characteristics through pattern recognition algorithms.

Legal Tech, which covers the three levels discussed in Chapter One of the monograph: 1.0, 2.0 and 3.0, refers to an extremely broad spectrum of applications within the legal sphere. Due to the fact that information technologies understood as Legal Tech 1.0., most often referring to the software supporting non-lawyer activities, have been used by both law firms and public entities (including law enforcement agencies) for a long time, the focus in this chapter will be on Legal Tech 2.0 and Legal Tech 3.0 tools, of which main guiding element is automation, and which differ mainly from one another by the level of the technological system autonomy.

## 2. *Possible Legal Tech Application by the Law Enforcement Agencies*

The indicated diversity of applications of technological tools would not allow conducting a legal analysis on their exploitation in the context of the law enforcement agencies work without making the necessary systematization. For this purpose, it should be pointed out that Legal Tech can be used by the law enforcement agencies for: 1) administrative and organisational activities and 2) substantive activities. The criterion for distinguishing between the above types of the services' activities results from their nature. The first group of activities relates to non-substantive, clerical activities, serving to improve the performance of the relevant tasks of law enforcement agencies. The second group includes overt and covert activities of the services aimed at the performance of tasks connected with the prevention and detection of criminal acts both in the course of preparatory proceedings as well as in an out -of -trial mode.

### 2.1. *Legal Tech on Administrative and Organisational Activities*

Application of Legal Tech with regard to the first type of law enforcement activity, i.e. administrative and organisational activities, can take various forms: from improving communication between entities involved in the criminal process (e.g. remote communication between the public prosecutor and the criminal court), through ensuring electronic circulation of documentation issued and processed by the services (paperless document management), to introducing tools that automate certain law enforcement ac-

tivities (such as drafting pleadings or dealing with notifications of crimes). Legal document automation software on the technological market[2] could easily be used in the administrative work of services to speed up and facilitate the preparation of standard and routine pleadings, statements or standard elements of records. Similarly, the work of law enforcement agencies would be facilitated by the widespread use of automatic speech recognition (ASR)[3] and optical character recognition (OCR)[4] systems, which would considerably speed up routine law enforcement activities, such as taking witness statements or processing information contained in historically produced paper documents. Some countries have also already embarked on innovative AI implementation projects within the law enforcement tasks: they have introduced police chatbots to provide security information and enable people to inform law enforcement agencies of suspected crimes, they have also developed mobile applications to reduce crime or started patrolling cities using robots[5].

---

2 Examples of this type of software include LISA (<http://robotlawyerlisa.com/>, accessed 08 February2021) or InteliLex (<https://www.intelilex.net/en>, accessed 08 February 2021).

3 For more on this subject see also: Dong Yu and Deng Li, *Automatic Speech Recognition* (Springer London Limited 2016); Biing-Hwang Juang and Lawrence R Rabiner, 'Automatic speech recognition – a brief history of the technology development' (2005) Georgia Institute of Technology. Atlanta Rutgers University and the University of California. Santa Barbara 67; Yi Ren, Xu Tan, Tao Qin, Sheng Zhao, Zhou Zhao and Tie-Yan Liu, 'Almost Unsupervised Text to Speech and Automatic Speech Recognition' (Volume 97: International Conference on Machine Learning, Long Beach, 9-15 June 2019) 5410.

4 For more on this subject see also: Arindam Chaudhuri, Krupa Mandaviya, Pratixa Badelia and Soumya K. Ghosh, 'Optical Character Recognition Systems' in: Arindam Chaudhuri, Krupa Mandaviya, Pratixa Badelia and Soumya K Ghosh (eds), *Optical Character Recognition Systems for Different Languages with Soft Computing, Studies in Fuzziness and Soft Computing Vol. 352* (Springer 2017) 9 – 41; Noman Islam, Zeeshan Islam and Nazia Noor, 'A Survey on Optical Character Recognition System' (2016) 10 Journal of Information & Communication Technology -JICT <https://arxiv.org/abs/1710.05703> accessed 8 February 2021.

5 Many examples of innovative applications of AI in the police operations are provided by the Dubai10X project, which is undergoing a technological transformation using artificial intelligence tools in the United Arab Emirates police force, among others (see Amira Agarib, 'Dubai Police unveil Artificial Intelligence projects, Smart Tech' (Khaleej Times, 12 March 2018) <https://www.khaleejtimes.com/nation/dubai/dubai-police-unveil-artificial-intelligence-projects-smart-tec>, accessed 08 February 2021; Rory Cellan-Jones, 'Dubai Police Unveil Robot Officer' (BBC, 24 May 2017) https://www.bbc.com/news/technology-40026940, accessed 08 February 2021.

All applications of technological tools in the field of administrative and organisational activities are intended to streamline and speed up the processing of cases. While changing the nature of traditionally efforts- and time-consuming activities, as a rule they do not change the basic way in which services perform their functions. The use of IT tools in the course of extra-legal activities, although important from the point of view of streamlining the functioning of services (and as a result valuable from the perspective of security of the whole society), does not revolutionise the philosophy of law enforcement agencies, and from the IT point of view does not differ from general technological trends prevailing in other sectors.

Business-oriented and non-legal applications may be here advantageously implemented by the law enforcement agencies without a significant risk of violating the basic legal and ethical principles governing the functioning of services. On the other hand, automation of substantive activities, including first of all investigative activities, which are within the core of law enforcement activities, takes on a completely different character.

### *2.2. Legal Tech in Substantive Activities*

While in the case of technological tools used in office activities it is rather impossible to state that such systems are dedicated to lawyers only and are characteristic solely for the legal industry (thus, this is not Legal Tech sensu stricto, but tech in general that is used just for the purpose of practicing law), within the scope of investigative activities at least some of the tools will be strictly dedicated for legal purposes or even the need to create them will arise directly from a specific demand of the services.

Although it is not possible - if only due to the constantly advancing technological development - to list exhaustively the areas in which law enforcement agencies currently use advanced Legal Tech tools in the course of their substantive work[6], it is required to divide them into four main categories of activities. These are: 1) crime prediction, 2) automation of the detection of crimes and their perpetrators, 3) automated analysis of

6 See also Ephraim Nissan's review of the tools (Ephraim Nissan, 'Digital technologies and artificial intelligence's present and foreseeable impact on lawyering, judging, policing and law enforcement' (2017) 32 AI & Society 441 – 464, more broadly on this subject Ephraim Nissan, *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation* (Springer 2012).

evidence, and 4) automation of decision-making processes in the course of investigations conducted by services.

### *2.2.1. Crime Prediction*

The idea of crime prediction is well known to the average citizen thanks to pop culture's ideas about punishing offenders before they commit a crime[7]. Modern predictive policing techniques primarily aim to automatically identify certain characteristics, events or persons, mainly to prevent crime, and often also to use the results of predictive policing in criminal proceedings[8]. Predictive policing includes four main categories of predictions based on advanced analytical techniques: methods for predicting crime (places and time periods with a higher risk of crime), methods for predicting offenders (people at risk of committing crime in the future), methods for predicting offender identity (matching likely offenders to past offences based on profiling), and methods for predicting victims of crime (identifying people potentially at risk of becoming a victim as a

---

7 The most famous example from the mass culture is the 2002 film „Minority Report", directed by Steven Spielberg, based on the short story of the same name by Philip K. Dick published in Fantastic Universe magazine in January 1956. Clearly, the predictions generated by modern systems have little in common with the predictions on which the story of "Minority Report" was based. Nowadays these are software based on statistical methods producing estimates of the future based on data from the past (collected by information services or publicly available databases). Prediction results are always probabilistic, never certain. For more on predictive policing see Andrew Ferguson, 'Predictive Policing' (2017) 94 Washington University Law Review 1109; Albert Meijer and Martijn Wessels, 'Predictive Policing: Review of Benefits and Drawbacks' (2019) 42 International Journal of Public Administration 1031.

8 See the case of Loomis v. Wisconsin, pending before the Supreme Court of the State of Wisconsin, United States of America (<https://caselaw.findlaw.com/wi-supreme-court/1742124.html>, accessed 08 February 2021). Eric L. Loomis in 2013 was arrested while driving a car that had been used earlier during the shooting. When he applied for parole, his profile was assessed by software called COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) used by US courts to assess the likelihood of recidivism (for more on how the system works, see the software developer's guide available at https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf, accessed February 2021). As the system indicated a high risk of recidivism against Eric L. Loomis, the court denied the possibility of parole and sentenced the applicant to six years in prison.

result of a criminal act)[9]. Crime mapping based on advanced risk analysis techniques is useful both from the point of view of resolving an individual case, as well as from the broader perspective of allocating human resources in service activities and determining overall law enforcement strategies. However, it is quite clear from this example that the use of certain IT tools by services is not only targeted at a small group of persons already identified as involved in criminal activities, but also - and perhaps above all - at the general public, from which cases with a specific criminal risk are "picked up"[10]. Recent, widely discussed cases of discovered discriminatory tendencies of predictive tools based on machine learning raise legitimate questions about the acceptability of using such tools in criminal cases[11].

### *2.2.2. Automated Detection of Crime and Offenders*

The second highlighted area of application of Legal Tech within the field of the law enforcement, i.e. automation of the detection of crimes and

9 Walter L Perry, Brian McInnis, Carter C Price, Susan C Smith and John S Hollywood, 'Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations' (2013) National Institute of Justice, Safety and Justice Program, RAND Corporation research report series XIV <https://www.rand.org/pubs/research_reports/RR233.html> accessed 8 February 2021.

10 Citing Rodney Monroe, currently retired police commissioner in Charlotte-Mecklenburg, North Carolina, United States: "We're not just looking for crime. We're looking for people" - quoted in Robert L. Mitchell, 'Predictive policing gets personal' (ComputerWorld, 24 October 2013) <https://www.computerworld.com/article/2486424/predictive-policing-gets-personal.html>,. accessed 8 February 2021.

11 See the report of the NGO ProPublica regarding the abovementioned COMPAS (Julia Angwin, Jeff Larson, Surya Mattu and Lauren Kirchner, 'Machine Bias' (ProPublica, 23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>accessed 8 February 2021), a także Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman and Aram Galstyan, *'A Survey on Bias and Fairness in Machine Learning'* (2019) arXiv preprint arXiv:1908.09635; Xue Songkai, Mikhail Yurochkin and Yuekai Sun, *'Auditing ML Models for Individual Bias and Unfairness'* (2020) 108 (PMLR 108/2020) Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics () 4552; Ellora Israni, 'Algorithmic Due Process: Mistaken Accountability and Attribution in State v. Loomis' (Jolt Digest, 31 August 2017), <https://jolt.law.harvard.edu/digest/algorithmic-due-process-mistaken-accountability-and-attribution-in-state-v-loomis-1> accessed 8 February 2021.

their perpetrators[12], is mostly based on techniques capable of extracting information from data (data mining). This can take the form of automated analysis of the anomaly (e.g. of thefts) based on data from CCTV footage in public spaces, automated examination of electronic money transfers to uncover money laundering, detection of child pornography based on analysis of online video material or ongoing examination of social media content to uncover hate speech[13]. The facial recognition systems, which enable the matching of a human face from a digital image or video frame to law enforcement databases of faces, are quite a specific case[14]. Such systems are widely used by security services in many countries, including a large part of the Member States of the European Union[15]. Some countries have also chosen to use facial recognition systems in real-time interventions by equipping service personnel with facial recognition goggles[16], an interesting combination of two technologies: a software facial recognition system and a hardware body cam i.e. a video recorder attached to the body or clothing of uniformed service personnel.

---

12 Clearly, most of the techniques set out in this paragraph can be successfully used not only to detect crimes and criminals, but also to obtain evidence in criminal cases.

13 See also Mohammad Reza Keyvanpour, Mostafa Javideh and Mohammad Reza Ebrahimi, 'Detecting and investigating crime by means of data mining: a general crime matching framework' (2011) 3 Procedia Computer Science 872.

14 The threats connected with the use of such tools to human rights had been promptly recognised by the Council of Europe, which has been active in regulating the use of automatic facial recognition tools ('Facial recognition: strict regulation is needed to prevent human rights violations' (CoE, 28 January 2021) <https://www.coe.int/en/web/artificial-intelligence/-/facial-recognition-strict-regulation-is-needed-to-prevent-human-rights-violations> accessed 8 February 2021).

15 Nicolas Kayser-Bril, *'At least 11 police forces use face recognition in the EU, AlgorithmWatch reveals'*, Algorithm Watch, 11 December 2019, updated 19 June 2020, <https://algorithmwatch.org/en/story/face-recognition-police-europe/> accessed 8 February 2021. The Polish Police uses a system called BriefCam that performs automatic analysis of video content to detect people, vehicles, etc. (Ewelina Kucharska, 'BriefCam - one system, many possibilities' (2019) 12 Stołeczny Magazyn Policyjny 20).

16 'Chinese police spot suspects with surveillance sunglasses' (BBC, 7 February 2018) <https://www.bbc.com/news/world-asia-china-42973456#:~:text=Police%20in%20China%20have%20begun,crowds%20while%20looking%20for%20fugitives> accessed 8 February 2021.

### 2.2.3. *Automatic Evidence Analysis*

The third area in which law enforcement agencies use Legal Tech tools in their substantive work is evidence analysis. These tools are of particular importance in the area of so-called e-discovery[17], i.e. the discovery of electronically stored information (ESI) during legal proceedings[18]. Various Legal Tech 1.0 tools can be used in e-discovery, including in the course of a criminal case, as this process primarily involves the collection and processing of electronic evidence. From the point of view of Legal Tech 2.0 and 3.0, however, technology-assisted review (TAR), which at the current stage of technological development is usually based on natural language processing (NPL) techniques and machine learning (ML) models, is of particular importance. TAR enables the effective analysis of a big number of data. In a world of Big Data, without such tools law enforcement agencies would rely on "manual" verification of electronic data, which would almost always result in drastically reduced effectiveness[19]. At the same time, it is important to remember that AI-based automated data analysis tools can be a very useful search assistant, identifying relevant data and sorting it, however it is impossible to assign the entire evidence proceedings to them. The success of AI-based e-discovery lies in the seamless collaboration between a human being and a system[20].

---

17 *Discovery - in common law countries it is a pre-trial procedure for gathering evidence. In the countries of the continental system, the actions aimed at establishing the circumstances in question are generally carried out in the course of an evidentiary procedure.*

18 *E-discovery has always been of interests to academics in the context of criminal law – see* Ken Strutin, 'Databases, E-Discovery and Criminal Law' (2008) 15 Rich. JL & Tech. 1; Justin P Murphy, '*E*-Discovery in Criminal Matters - Emerging Trends & the Influence of Civil Litigation Principles' (2010) 11 Sedona Conference Journal 257; Jenia Turner, 'Managing Digital Discovery In Criminal Cases' (2019) 109 The Journal of Criminal Law and Criminology 237.

19 Maura R Grossman and Gordon V Cormack, 'Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review' (2010) 17 Rich. JL & Tech. 1; Herbert L Roitblat, Anne Kershaw and Patrick Oot, 'Document categorization in legal electronic discovery: computer classification vs. manual review' (2010) 61 Journal of the American Society for Information Science and Technology 70.

20 See Michael Mills, 'Artificial Intelligence in Law: the State of Play 2016', Thomson Reuters, 4, https://britishlegalitforum.com/wp-content/uploads/2016/12/Keynote-Mills-AI-in-Law-State-of-Play-2016.pdf, accessed 8 February 2021.

### 2.2.4. Automating Decision-Making Processes

However, Legal Tech tools need not only be of an assistance for the personnel of the law enforcement agencies. In certain instance they can participate in decision-making processes carried out in the course of proceedings, and even take over the role of an independent decision-maker. The fourth of the highlighted areas of application of Legal Tech tools in the work of services is automation of decision-making processes in the course of conducted proceedings. The use of Legal Tech tools for the purposes of algorithmisation of the process of law application has already been discussed from the theoretical point of view in part II of this monograph. Incorporating these considerations into the practice of law enforcement agencies, it should be noted that in this case we will be dealing with automation of a potentially wide range of decisions[21]. Although one might be of the opinion that such a level of automation of proceedings conducted by law enforcement agencies has not become yet a standard, it has in fact been used in practice for years, e.g. in automatic traffic surveillance systems. For instance, CANARD[22] has been operating in Poland since 2011 which due to the automatic registration of offences reports violations of regulations within the scope of exceeding the established speed limits and disobeying traffic lights by the drivers. Information sourced from the point and section speed measuring devices or monitoring of intersections are processed automatically by the Central Processing System and then verified by the system in terms of the possibility of their further processing and use as evidence in a case of a traffic violation. The system also automatically exchanges information with the Central Register of Vehicles and Drivers, which makes it possible to send an automatic request to identify the driver of the vehicle. After receiving (or failing to receive) an answer from the vehicle owner, the system creates another solution such as: issuing a fine, delivering a statement to a person indicated

21 Both those which take the form of a formal procedural decision (e.g. the system, on the basis of the analysis of data concerning the offence and the suspect, decides that it is appropriate to issue a decision on bail rather than to apply to the court for temporary arrest) and those which do not take any particular procedural form (e.g. the system, after the analysis of the database of inhabitants of a given city, selects persons who could potentially be the perpetrators of an offence and then automatically recognises their faces on public surveillance recordings, locating them for the law enforcement agencies).

22 The Automatic Road Traffic Supervision Centre (CANARD) is an organisational unit of the General Inspectorate of Road Transport established to supervise road traffic.

by the owner or referring the case to court[23]. Employees of CANARD supervise the correctness of the whole procedure, however, as a rule, the system automatically performs all actions necessary to issue a summons.

It should be assumed that with the development of Legal Tech tools (especially those based on ML and NLP) the scope of their autonomy will increase. This will inevitably result in more and more significant interference in the scope of data regarding citizens processed by law enforcement agencies and, what is more important, will increasingly allow for automation of decisions made by law enforcement agencies with regard to citizens. For this reason, it is necessary to determine a legal framework for such actions.

### *3. Legal Tech in Law Enforcement - a Regulatory Perspective*

The undisturbed functioning of most of the methods in which Legal Tech tools are used in the work of law enforcement agencies set out in this chapter relies on ensuring automatic analysis of data held by the services. This can contribute both to speeding up and improving the quality of law enforcement investigations and, more generally, to better managing of the public security. However, these data remain to a large extent personal data. Taking into account the fact that the activities of law enforcement services - as it has been mentioned in this chapter - are aimed at a very wide range of citizens - not only those who are in any way involved in criminal activities, but also those who have never had and will never have any contact with the criminal world, one of the most important axis of legal considerations in this area are the legal regulations related to the protection of natural persons in relation to the processing of personal data by competent authorities for broadly defined criminal purposes[24]. Importantly, the general regulations on personal data would not be applicable within this

23 <https://www.canard.gitd.gov.pl/cms/> accessed 8 February 2021.

24 Obviously, this is not the only legal perspective that can be analysed in terms of the use of Legal Tech tools in the work of uniformed services. Equally important as personal data protection regulations remain the fundamental rights, which are not the topic of this chapter. In this respect, however, see: European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights, PE 656.295, 2020, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU> (2020)656295_EN.pdf, accessed 8 February 2021.

scope[25]. On European level[26], the relevant law remains Directive 2016/680 of the European Parliament and of the Council of 27 April 2016[27], hereinafter referred to as the "LED Directive"[28].

As rightly highlighted in recital 3 of the preamble of the LED Directive, a rapid technological development and globalization have brought new challenges within the field of personal data protection, increasing the scale of collection and cross-border exchange of personal data by law enforcement agencies. Technology now makes it possible to process personal data[29] on an unprecedented scale for activities such as the prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties. The LED, seeking a balance between the free movement of personal data between EU Member States' services for criminal purposes while ensuring effective police cooperation and the

---

25 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals 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) [2016] OJ L119/1, hereinafter referred to as "GDPR". As regards the exclusion of the application of the GDPR as to the protection of natural persons in relation to the processing of personal data by competent authorities in the framework of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including for the purpose of protecting against and preventing threats to public security, see Recital 19 GDPR. For more on the scope of the GDPR and the LED see Juraj Sajfert and Teresa Quintel, 'Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities' in Mark Cole and Franziska Boehm (eds), *GDPR Commentary* (Edward Elgar Publishing 2020) 3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3285873>, accessed 8 February 2021.

26 Those interested in non-EU, US regulation are referred to, inter alia: Reema Shah, 'Law Enforcement and Data Privacy - A Forward-Looking Approach' (2015) 125 Yale Law Journal 543.

27 Directive (EU) 2016/680 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 by competent authorities for the purposes of prevention, investigation, detection and prosecution of criminal offences or the execution of criminal penalties, on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ L119/89. The LED Directive, similarly to the GDPR, was adopted in May 2016, together representing an important step forward in establishing a comprehensive EU data protection regime. It can be seen both as a lex specialis to the GDPR and a completely independent parallel regulation (Mark Leiser and Bart Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680' (2019) 5 European Data Protection Law Review 367).

28 Abbreviation for Law Enforcement Directive.

29 This includes any information about identified or identifiable natural persons (see Article 3(1) LED).

due protection of the fundamental rights and freedoms of individuals, introduces an equivalent level of protection of personal data used in the field of criminal policy[30] and common rules for monitoring compliance with and enforcement of the binding principles[31].

The processing of personal data[32] under the LED must comply with the fundamental principles governing data protection law, i.e. lawfulness, fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality[33] as well as accountability[34]. These rules are broadly in line with the general principles of the GDPR[35], with one important exception relating to transparency. Indeed, Article 4(1)(a) of the LED - contrary to Article 5(1)(a) of the GDPR - does not provide for an obligation to process personal data in a way which is transparent to the data subject. On the one hand, the lack of transparency is justified by the nature of the activities carried out by the services[36], but on the other hand, one may not forget that these activities often concern a basically unlimited circle of citizens. It is also worth highlighting a certain inconsistency in the text of the Directive - although Article 4(1) of the LED Directive does not mention the principle of transparency in its content, recital 26 of its preamble indicates that „the processing of personal data must be (...) transparent in respect of the individual concerned (...). This does not prevent law enforcement agencies from carrying out activities such as covert surveillance or video monitoring".

---

30 It should be borne in mind that Article 1(3) LED does not preclude Member States from providing higher safeguards to protect the rights and freedoms of data subjects.

31 Examples of EU regulations implementing Article 11 LED, may be found in Matthias Hudobnik, 'Data protection and the law enforcement directive: a procrustean bed across Europe?' (2020) 21 ERA Forum 21 489.

32 The processing of personal data by competent authorities referred to in the LED encompasses a broad category of operations on data. According to Article 3(2) and Recital 34 of the LED, this includes any operation or set of operations which is performed upon personal data or sets of personal data within the scope of the Directive by automated or non-automated means, including in particular the collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, alignment or combination, restriction of processing, erasure or destruction, as well as the transmission of personal data, which serves the purposes specified in the LED, to recipients who are not subject to it.

33 Article 4(1) LED.

34 Article 4(4) LED.

35 Article 5(1) GDPR.

36 Full transparency could hinder or even frustrate the objectives of the investigation carried out by the competent services (Leiser and Custers (n 27) 371).

In the context of the application of Legal Tech tools within the law enforcement agencies' operations presented in the chapter, one of the most relevant provisions of the LED Directive remains Article 11 on automated decision-making in individual cases[37]. According to this provision Member States shall ensure that decisions which are based solely on automated processing, including profiling[38], and which produce an adverse legal effect for the data subject or significantly affect him/her, shall be prohibited[39]. An exception to such prohibition shall only be allowed if such automated decisions are permitted by the EU law or a national law of the Member State to which the controller is subject, and at the same time the law provides for suitable safeguards with respect to the rights and freedoms of the data subject, including at least the right to obtain human intervention from the controller[40]. Member States - apart from the right to obtain human intervention imposed by the Directive - are left free to establish ap-

37 This is a similar, but not identical, regulation to Article 22(1) GDPR. An intriguing difference between the LED regulation and the GDPR remains the fact that the prohibition of automated processing in the GDPR applies to decisions that "produce legal effects on the data subject or otherwise materially affect him or her in a similar manner" (cf. Article 22(1) GDPR), while the LED Directive prohibits in principle only decisions that "produce an adverse legal effect on the data subject or seriously affect him or her" (cf. Article 11(1) LED).

38 According to Article 3(4) LED, „profiling" means any form of automated processing of personal data that involves the use of personal data to evaluate certain personal factors relating to an individual, in particular to analyse or predict aspects relating to the individual's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movement. Criminal prediction, discussed earlier in the chapter, relies to a large extent specifically on profiling. It is also worth pointing out that although profiling and automated decision-making may be combined activities within the same process, they can also be carried out separately. There may be cases of automated decisions made with the use of profiling (or without) and profiling taking place without automated decision-making (Article 29 Working Party, Opinion on some key issues of the Law Enforcement Directive (EU) 2016/680, 29 November 2017, 17/PL, WP 258, 14 <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178> accessed 8 February 2021.

39 At the same time, it should be borne in mind that even where the automated processing of personal data by law enforcement agencies does not fall within the scope of Article 11 LED, i.e. where it is not prohibited in principle (primarily because the processing will not be wholly automated or will not produce adverse effects for the data subject), a number of other provisions of the Directive shall apply to it (see Articles 4, 8, 10, 13 - 17 LED).

40 For more on the transposition of the LED provisions into national legal orders see <https://eur-lex.europa.eu/legal-content/PL/NIM/?uri=CELEX:32016L0680> accessed 8 February 2021.

propriate safeguards for the automation of decisions. Recital 38 of the LED Directive, however, indicates in this respect – similarly to the provisions of Article 22 and Article 15 of the GDPR - the required safeguards, in addition providing for the following: information obligations towards the data subject and the right to express one's opinion, obtaining an explanation of the decision and a right to contest it[41]. Due to the non-binding nature of the preamble, these can only be regarded as guidelines for national legislators[42].

The prohibition of automated decision-making is even stricter when it comes to the processing of specific categories of data[43] which are not uncommon in the course of the services' operations. To the extent indicated, a decision may be automated only if "suitable measures have been implemented to safeguard the data subject's rights, freedoms and legitimate interests"[44], and in any case no such decision may be made, based on profiling which would result in discrimination against individuals[45] (in line with the wording of Article 21 of the Charter of Fundamental Rights[46]). The exclusion of the consent as a basis for automation within the police context remains the main difference between the LED Directive and GDPR regulations when it comes to the automated decision making[47]. As recital 35 of the LED Directive rightly indicates, the consent of the data subject should not constitute a legal basis for the processing of personal data by competent authorities for criminal purposes. Indeed, if the data subject has to comply with a legal obligation (which is usually the case regarding the procedural position of persons involved in pre-trial investigations), he/she does not have effective freedom of choice which is the essence of the free consent. As the Working Party rightly points out -Article 29, the clear imbalance between the rights of the data subject and

41 One may reflect on the reasons why the EU legislator did not decide to explicitly include the right to express one's position and the right to contest the decision in the text of Article 11 LED, following the example of the regulation of Article 22(3) GDPR.

42 Compare also: Juraj Sajfert and Teresa Quintel (n 25) 10.

43 This includes personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation (Article 10 LED).

44 Article 11(2) LED.

45 Article 11(3) LED.

46 Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

47 Compare Article 22(2)(c) and Article 22(4) GDPR.

the rights of the controller (law enforcement agency), rules out the consent as a basis for processing in this regard[48].

### *4. Summary*

Although the common perception is that new technologies reduce the time spent on cases and free the service employees from some performing some time- and effort -consuming activities, surveys conducted all over the world concerning the use of new technologies within the police operations demonstrate that assessments of the effectiveness of the applied technological solutions are extremely rare; therefore, hard empirical data on whether new technologies within the police operations actually work are very limited[49]. However, research shows that the use of Legal Tech tools within the law enforcement agencies' work is generally welcomed by the uniformed services, although at the same time there are also views that IT tools limit the discretion of human decision-makers[50]. It is not unlikely that the development of Legal Tech 3.0 tools, increasing the level of automation when it comes to the substantive work of the law enforcement agencies, will strengthen the officers' convictions on the reduction of their independence in decision-making processes, at the same time raising concerns about entrusting the tasks excessively to the technological systems. The key to responsible use of advanced Legal Tech solutions by the services thus involves primarily:

1) precise identification of areas where automation would bring more benefits than it would generate potential risks,
2) appropriate determination of the competence of persons using the technologies (not only technological knowledge, but above all legal and ethical awareness) and
3) implementation of well -designed legal solutions in this area.

---

48 Working Party Article 29, Opinion on some key issues of the Enforcement Directive (EU) 2016/680, 29 November 2017, 17/PL, WP 258, <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610178> accessed 8 February 2021.

49 Bart Custers and Bas Vergouw, 'Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies' (2015) 31 Computer Law & Security Review 518.

50 Janet BL Chan, 'Technological Game: How Information Technology is Transforming Police Practice' (2001) 1 Criminal Justice: The International Journal of Policy and Practice 139.

Interestingly, in the studies on the practical functioning of police services, apart from obvious difficulties in the implementation of IT tools in the operations of the services (such as insufficient funds for the purchase of technology or technological deficiencies of the tools themselves), the following factors are mentioned as barriers to the use of Legal Tech: lack of appropriate legal solutions, insufficient clarity thereof and difficulties in the appropriate processing of personal data[51]. It seems, therefore, that technological development alone is not the only determinant of the efficient and secured implementation of technological tools within the law enforcement agencies' operations. Legislative efforts[52], constant education of officers within this field and ongoing monitoring of the effectiveness of the tools used are equally important.

51 ibid 523.

52 The idea of certification of AI tools used in the sphere of justice (European Commission for the Efficiency of Justice) deserves recognition in this respect CEPEJ, 'Possible introduction of a mechanism for certifying artificial intelligence tools and services in the sphere of justice and the judiciary: Feasibility Study', 8 December 2020, CEPEJ (2020) 15 Rev).