UDK 343:621.39
Review article

MEMORIES OF THE FUTURE: SWEETIE AND THE IMPACT OF THE NEW TECHNOLOGIES ON THE CRIMINAL JUSTICE SYSTEM

Laura Stănilă, PhD, Senior Lecturer
West University Timișoara, Faculty of Law
Timișoara, 9A Eroilor de la Tisa Bvd., jud. Timiș, Romania
laura.stanila@e-uvt.ro

ABSTRACT

The new age of technology has made its mark on all dimensions of social life. The justice system did not escape this influence, currently facing the need to adapt its principles and standards of criminal justice as a result of using Artificial Intelligence in the criminal investigation phase as well as in other stages of the criminal process. "Sweetie" is by far one of the most disputed means of criminal investigation that puts both the theory and the criminal procedural practice to the test.

Through this interdisciplinary study we propose an analysis regarding the new means of investigation, trying to identify the advantages and disadvantages of using new technologies in the criminal trial, with a detailed description of the instrument "Sweetie" and of some cases in which it was used.

***Keywords**: Sweetie, Criminal investigation, Criminal justice system, Artificial Intelligence, Preparatory acts, Criminal attempt*

1. NEW TECHNOLOGIES AND THE CRIMINAL INVESTIGATION. THE NEED FOR ADAPTATION

The investigative phase of the criminal process is of utmost importance since, during it, evidence is gathered by the judicial organs in order to support accusations and prove criminal conduct and culpability. Being such a difficult process and requiring extreme care, perseverance and much attention to detail, it consumes time, human and financial resources. At the same time, humans involved in this process, depending on the amount of work and quantity of data they need to analyze, are exposed to error, and errors are difficult and costly to be removed and

repaired. As stated in the doctrine, "especially in large crime investigations, investigators are faced with a mass of unstructured evidence of which they have to make sense. They have to map out the possible hypotheses about what happened and assess the potential relevance of the available evidence to each of these hypotheses". [1]

Facing all these issues, the law enforcement agents need to find ways, tools and means to ease their work and achieve expected results in the fight against the crime phenomenon. These new ways could be based on Artificial Intelligence (AI) and telematic tools as they could meet the standards of rapidity, objectivity and efficiency. "Software could offer such tools by supporting crime investigators in expressing their reasoning about a case in terms of arguments on the relevance of evidence to the various hypotheses using common knowledge. In the current practice of crime investigation and similar fact-finding processes, software for managing and visualizing evidence is already being used"[2].

Specific forms of crime which are number increasing are critically linked to internet and online tools to be committed, thus the investigator should use similar tools in order to discover and catch the perpetrators. One example is child pornography, which tends to become a dangerous global phenomenon. It was stated that, at any time of the day, an estimated 750,000 men are looking for online webcam sex with children[3]. Facing this huge number of perpetrators, the law enforcement agents cannot rely solely on the current methods of detection and on the reporting by the victims. Even if they could appeal to undercover operations, it is utopic to expect significant results while human and financial resources are limited while the speed of state reaction is essential. In these troubled times state agents need to show imagination, be creative and use the best of the existent tools in the fight against crimes. Such a creative example is Sweetie – a chatbot that could be the best way of discovering crimes of child pornography without human victims and before any perpetrating acts are committed. Creation and use of such novel tools is conditioned by the acceptance of the policy makers and the cooperation between them and the private sector which is the main actor in the Artificial intelligence domain but focused solely on profits. "As long as outdated views of policy makers on crime prevention and profit-centered approach of the private sector

---

1 Bex, F. *et al., Sense-making software for crime investigation: how to combine stories and arguments?*, Law, Probability and Risk, *vol.* 6, issue 1-4, March 2007, pp. 145–168, [https://doi.org/10.1093/lpr/mgm007], accessed 13. April 2020

2 *Ibid.*, p.146

3 [https://www.savesweetienow.org], accessed 13. April 2020

prevail over unconventional methods of fighting crimes, these types of theoretical solutions are doomed to stay on paper". [4]

2. FUTURISTIC METHODS OF CRIME DETECTION

In the context of new ways of committing crimes arising, with technological and transnational components, it is imperative for the law enforcement agents to adapt and use adequate means of investigation, as stressed in the first section of the present study. Reluctance for innovative tools and approaches and deferment in using Artificial Intelligence algorithms could dramatically affect the criminal investigation and allow perpetrators to escape criminal consequences.

Thus, the scholars have been preoccupied to identify futuristic methods and tools for crime detection, anchored in the new technological dimension of crime phenomenon. Until now, several AI methods are currently trialed and used in the investigative phase: chatbots, Big Data analysis by VoIP companies, specific software used to manage evidence or block the spread of crime forms[5].

2.1. Chatbots

A chatbot is a software application used to conduct an online conversation (text or speech) instead of providing direct contact with a live human agent[6]. The chatbot is designed to simulate human behavior in a conversation and typically requires continuous adjustment and testing. Chatbots are usually used for various purposes: customer service, request routing, information gathering and lately, their area of use has widened to crime investigation and identification of potential perpetrators of crimes.

Chatbots have evolved from totally dependent devices of human actors to almost independent software. As dependent to human actors, chatbots are "puppets" manipulated by humans, thus their "conduct" is the conduct of the human operator. Automated chatbots act independently and learn from their own experience and could create new crime prevention strategies. However, not even the latest ver-

---

4 Açar, K.V., *Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection*, International Journal of Cyber Criminology, January – June 2017, *vol.* 11, no. 1, p. 98–109, [DOI: 10.5281/zenodo.495775], accessed 13. April 2020

5 K.V. Açar (*ibid.*) points out three futuristic methods for crime detection: 1.Fully automated chatbots; 2.Big Data Analysis of Metadata by VoIP companies and 3.Big Data Analysis of Content Data by VoIP Companies.

6 Crăciun V., *Ce este un chatbot?* ["What is a chatbot?"], Today Software Magazine, Nr. 72, 2018, [https://www.todaysoftmag.ro/article/2645/ce-este-un-chatbot], accessed 15. April 2020

sion of Sweetie – Sweetie 2.0 - is a fully automated chatbot, still could be a very useful, tool in criminal investigation. By far, Sweetie chatbot experiment[7] of Terre des Hommes Netherlands is a remarkable example of how this simple principle can be applied in the fight against specific forms of crime such as virtual child pornography.

The scholars have stated that chatbots could be used as undercover agents. While the initial version of human dependent chatbots is perfectly compatible with the undercover agent actor, the advanced independent versions are unfortunately non, since they are non-human actors. "(…) A human being seems a necessary element of undercover investigations at the moment. However, in the proposed approach, humans would only involve in the evaluation of stored communications between chatbots and potential offenders, not during undercover operations. The legal framework for online child sexual abuse investigations should be changed to conduct such humanless undercover operations".[8] The use of undercover agents is strictly provided by the law which states on the characteristics, conditions and situations when such an exceptional investigative method could be used. The advanced version of Sweetie is actually a hybrid model of chatbot, not entirely independent of human actor. In the future, there are projects to develop a fully automated chatbot that could eliminate the human factor, only raising serious questions on the legality of the use of such method in the criminal process.

2.2. Big Data Analysis by VoIP companies

Voice-over-IP (VoIP) is an efficient method to communicate. VoIP involves sending voice transmissions as data packets using the Internet Protocol (IP), whereby the user's voice is converted into a digital signal, compressed, and broken down into a series of packets. The packets are then transported over private or public IP networks and reassembled and decoded on the receiving side.[9]

VoIP companies run two types of Big data analysis: analysis of Metadata and analysis of Content data.

a) Metadata is in fact Data that provide information about other data, summarizing basic information about it, making finding and working with particular

---

7 See short video on *Sweetie* at [https://youtu.be/aGmKmVvCzkw?t=10], accessed 13. April 2020

8 Açar, *op.cit.*, note 4, p.103

9 Varshney, U. *et al., Voice over IP*, Communications of the ACM, *vol.* 45, no. 1, 2002, p. 89, [https://dl.acm.org/doi/10.1145/502269.502271], accessed 15. April 2020

instances of data easier. In other words, Metadata is a shorthand representation of the data to which they refer.[10]

Metadata shows some attributes of communications such as date, creator and IP addresses without severely compromising the privacy of communications. Therefore, collecting metadata is easier both technically and legally since it takes up less space on disk and involves less intrusive personal information than the content data have. This method is used to detect possible online child pornography and other types of crimes/offenses which could be committed through internet by a pattern analysis of the metadata of VoIP communications (location, source, IP) that could lead investigators to potential victims or perpetrators. [11]

For example, a pour child from a minor victims "traditional provider" country contacts offenders from different countries during a limited period of time (one week). In this case VoIP company reads the "signals" - a resident of a very poor city chats with multiple foreigners from relatively wealthier countries - and after discloses the IP addresses and other helpful information like email addresses to the law enforcement authority for further investigations.[12]

b) Content data analysis exposes specific information of the VoIP communications between parties: texts, audio, video files and is highly intrusive. It requests legal authorizations and trained operators. An analysis of Skype which is used by millions of people worldwide to communicate shows that specific features of it – like real time translation[13]. In order to detect online child pornography for example, a content analysis could use code words like sexual meaning words in order to reveal suspect behaviors. When the results of such an analysis are corroborated with other data like type of money transfer (ex. PayPal, bitcoin) and location of IP, the final result might be extremely useful for the crime investigators.

2.3. Software expressly designed to be used in investigative phase of criminal process

There are many examples of software expressly designed to be used in investigative phase of criminal process. Analyst's Notebook by IBM[14] and HOLMES

---

10 Hare, J., *What is metadata and why is it as important as data itself?* Opendatasoft, 25 August 2016, [https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data], accessed 15. April 2020

11 Açar, *op.cit.*, note 4, p.103

12 *Ibid.*, p.104

13 *Ibid.*, p.105

14 [https://www.ibm.com/security/intelligence-analysis/i2/law-enforcement], accessed 15. April 2020

2[15] are both designed in 2006 and used in United Kingdom while Netherlands experimentally used BRAINS in crime investigation with some success in 2004. FLINTS[16] is another example which was first used by the British police in 1999 to manage forensic evidence.

Microsoft Company has created software that matches photos, even if they've been altered that is used in child pornography investigation, in order to help investigators to focus on new images surfacing online. Another software, Adobe Systems' Photoshop, is used to identify child pornography victims with tools that sharpen pictures to reveal clues.

Other initiatives using Artificial Intelligence are related to Google, which blocks search terms related to child pornography and to Thorn, a foundation supported by Hollywood actors which has created a database for tracking known child sex-abuse images and taking them offline.[17]

As stressed by the scholars, even if these software programs are extremely useful in the investigative phase, the results of the criminal investigation are "wholly dependent on human reasoning, and the structures resulting from such reasoning cannot be recorded and analyzed by the software"[18].

3. A CONTROVERSIAL INVESTIGATIVE TOOL: SWEETIE

As previously explained, Sweetie is a chatbot, an AI program, designed to combat online pedophilia (webcam sex with children) and to help identify suspects, perpetrators and victims. It was created by the organization Terre des Hommes[19] from Netherlands in 2013. Since its first use in 2013, Sweetie had led to the conviction of several English, Danish, Dutch and Belgian citizens for webcam sex with children.[20]

---

15 HOLMES 2 (Home Office Large Major Enquiry System) is an information technology system used by United Kingdom Police in order to facilitate murder and high value fraud investigations. It was developed by Unisys under the Private Finance Initiative. The name of this tool refferes to the Arthur Conan Doyle's character Sherlock Holmes. Further information can be retrieved from [http://www.holmes2.com/holmes2/index.php] aaccessed 13. April 2020

16 Nissan, E., *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation*, *vol.* 1, Springer, 2012, p.767-836. As regards FLINTS (Forensic-Led Intelligence System) and its benefits, also see Jackson A.R.W.; Jackson J.M., *Forensic Science,* second edition, Pearson, 2008, p. 7

17 Schweizer, K., *Avatar Sweetie exposes sex predators*, The Age, April 26, 2014, [https://www.theage.com.au/world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html], accessed 13. April 2020

18 Bex *et al., op.cit.,* note 1, p.146

19 Oficial site: [www.terredeshommes.nl], accessed 15. April 2020

20 Terre des Hommes, *First conviction for child abuse in Belgium thanks to Sweetie*, 9/04/2015, [https://www.terredeshommes.nl/en/news/first-conviction-child-abuse-belgium-thanks-sweetie], accessed 13. April 2020

In its first version - Sweetie 1.0 – the chatbot appeared as a virtual 10–year old girl from Philippine - was used to identify and expose pedophiles engaged in webcam sex tourism and was operated by a human agent. The conversations with the pedophiles were conducted by the human police agent, Sweetie being only its avatar. Despite its initial success, the use of Sweetie was limited by it being operated by a human actor who could conduct a limited number of online conversations at the same time. The number of suspects – sex solicitants - per hour was over 2000! In order to solve this problem, Sweetie 2.0 was created, a more advanced version of the chatbot. According to Schermer, Georgieva, Van der Hof and Koops, "the main difference with Sweetie 1.0 is that Sweetie 2.0 is no longer operated by a human, but is now a fully autonomous artificial intelligence that can engage in a meaningful conversation with a suspect"[21]. However, these authors are not entirely right, since Sweetie 2.0 is actually a hybrid model of chatbot, not entirely independent of human actor. In the future, there are projects to develop a fully automated chatbot that could eliminate the human factor, however, it would raise serious questions on the legality of the use of such method in the criminal process.

The main advantage in using Sweetie is that investigators can directly interact with pedophiles without putting anyone in danger, in other words, there are no potential victims, but only potential suspects. It is almost like discovering a crime before it was committed. As enthusiastic as could be, someone could not but observe that there are serious legal issues in relation with the "deeds" discovered by Sweetie: there is no crime/offense, no victim, and thus criminal law could not be imposed to anyone! In order to punish "sex predators" as a result of using Sweetie, further legislative interventions are necessary, for example, interacting with Sweetie must be qualified by law as criminal behavior.

"If this is not the case, then it will be much harder, if not impossible to prove that the suspect committed or attempted a criminal act. This in turn will make it more difficult to justify the use of Sweetie as an investigative method".[22]

Using Sweetie as an investigative method was praised by the civil society and questiond by the legal experts. Since Sweetie was designed and developed by a non-profit organization, despite its noble goal, European Policing Agency Europol has expressed reservations about its use: "We believe that criminal investigations using intrusive surveillance measures should be the exclusive responsibility of law enforcement agencies," spokesman Soren Pedersen told the Reuters news agency.[23]

---

21 Schermer, B. W. *et al., Legal Aspects of Sweetie 2.0*. Leiden/Tilburg: TILT, 2016, p. 10

22 *Ibid.,* p. 12

23 Crawford, A., *Computer-generated ‚Sweetie' catches online predators*, BBC News, 5 November 2013, [https://www.bbc.com/news/uk-24818769], accessed 13. April 2020

4. ISSUES REFERRING TO THE USE OF SWEETIE IN THE CRIMINAL PROCESS

As Sweetie fame was raising, it became subject for a very detailed legal analysis that led to the conclusion it does not meet the law requirements for a recognized investigative tool[24]. The Report was published in 2016 and demoralized the enthusiastic supporters of Sweetie.

The main issues found by the researchers were:

a) Lack of human element

The advanced Sweetie 2.0 is no longer operated by a human, but an autonomous Artificial Intelligence algorithm that can engage in a conversation with a suspect. If we embrace the idea of Sweetie being an undercover agent, the lack of human operator is the element that eliminates the possibility of using Sweetie as such. Since domestic criminal procedure legislations regulate undercover agents as human beings, then nothing is to be said in this direction.

b) Ethical issues regarding the non-human nature of Sweetie. The concept of "virtual victim"

Because Sweetie is an avatar, a virtual character, programmed to appear and talk as a child but clearly no real child is ever involved in the process, and because no sexually explicit behavior on the part of the "victim" takes place[25], questions were raised if there is an actual victim in this case. The concept of victim is only understood in connection with a human being, since only human beings are subject for criminal protection, exercise rights and are holders of the social values protected by the criminal law.

This conclusion raises another question: could Sweetie be considered a virtual victim and if so, what is a *virtual victim*? If we are comfortable with this new category, we may proceed further.

Baarfield and Blitz propose to distinguish between virtual sexual assaults involving avatar interactions and those using immersive interactions and go even further using new terms such as *virtual victim* and *virtual perpetrator*[26] They even distinguish between fully virtual sexual interactions and combined sexual interactions between humans using avatars or between humans and virtual agents. Also they

---

[24] Schermer, *et al., op.cit.,* note 21, pp. 82-86

[25] *Ibid.,* p. 29

[26] Baarfield W.; Blitz, M.J., *Research Handbook on the Law of Virtual and Augumented Reality*, Edward Elgar publishing, 2018, p. 368

distinguish between virtual reality and immersive reality[27]. Such an analysis is of great importance to understand the type of interaction in case of Sweetie and the human sexual predators.

A virtual perpetrator is, in fact, a virtual agent committing a crime. The virtual agent could be an avatar of a real person, a chatbot or a genuine virtual agent (a more advanced software than the one used to create a chatbot, which has abilities and skills exceeding those of chatbots, being improved with NLP – natural language processing[28]).

As shown in the table below, the first version of Sweetie - Sweetie 1.0 - could be qualified as a *human victim* - human user virtually sexually assaults an avatar controlled by another human being, using an avatar, while the interraction between the two is an avatar interaction with human perpetrator. In this case Sweetie is only an AI tool while the human operating it is an undercover agent. The situation could be legallyjustified by extensively interpreting existing criminal procedure regulation concerning undercover agents.

The second version of Sweetie - Sweetie 2.0 -, being an almost independent entity which was only designed and programmed by a human, while acting independently, could be a *virtual victim* - human user virtually sexually assaults a wholly virtual agent using an avatar. In this case Sweetie itself is an undercover agent acting as a victim in order to expose criminal conduct of the human perpetrator.

	Avatar - interaction	**Immersive - interaction**
Human Perpetrator	*Virtual victim:* human user virtually sexually assaults a wholly virtual agent using an avatar. *Human victim:* human user virtually sexually assaults an avatar controlled by another human being, using an avatar.	*Virtual victim:* Human user virtually sexually assaults a wholly virtual agent using immersive tech. *Human victim:* Human user virtually sexually assaults a virtual agent controlled by another human being using immersive tech.

[27] Immersive technology refers to technology that attempts to emulate a phisical world through the means of a digital or simulated world by creating a surrounding sensory feeling, thereby creating a sense of immersion, enabling mixed reality. Immersive reality is a combination of Virtual reality and Augmented reality or a combination of physical and digital. See short video Tiffany Lam, How immersive technologies (AR/VR) will reform the human experience, TEDxQueensU, on [https://www.youtube.com/watch?v=Fi97-DAcGMk], accessed 15. April 2020

[28] Kidd, C., *Chatbot vs Virtual Agent: What's The Difference?,* BMC Blogs, 27 November 2019, [https://www.bmc.com/blogs/chatbot-vs-virtual-agent/], accessed 05. June 2020

Virtual Perpetrator	*Virtual victim:* wholly virtual avatar is virtually sexually assaulted by a wholly virtual agent. *Human victim:* avatar controlled by a human being is virtually sexually assaulted by a wholly virtual agent.	*Virtual victim* – n/a this interaction is not distinct from an interaction between two wholly virtual avatars since the immersive tech only applies to fuse the real - world with the virtual world. *Human victim:* human user virtually sexually assaulted by a wholly virtual agent controlled by another human being while wearing immersive tech.

The perpetrator-victim interraction in the virtual space (Table 1.)

From an ethical perspective, Sweetie's most important feature is the fact that it does not put actual children at risk[29] – but this feature is in the same time its main flaw: in most criminal law systems, a real victim is mandatory in order to indict a suspect for committing a criminal deed. The law in force does not recognize virtual victims….yet! (?)

c) Issues regarding criminal nature of the acts committed by the perpetrator

Because Sweetie does not involve in sexually explicit behavior or nudity acts, the animations of Sweetie cannot be qualified as child pornography. As a result, the human actor interacting with Sweetie cannot complete the offence of accessing (and possibly storing) child pornography. From a law enforcement perspective this is an issue, given that in most countries accessing (virtual) child pornography would be the go-to offence in the case of Sweetie[30].

The imposition of criminal liability for an attempted sexual offense in the case of interacting with Sweetie is conditioned by the criminalization of those acts by the national legislator.

d) lack of procedural criminal provisions

Sweetie is an AI tool developed to facilitate the investigative actions of the judicial bodies, and would operate on public online platforms in an independent manner (Sweetie 2.0.). "The chatbot/avatar will be used as a lure for the alleged offender, but will also be capable of interacting with the suspect and recording and storing their interactions as well as available information on the offender, such as for

[29] Schermer *et al., op.cit.,* note 21, p. 29

[30] *Ibid.,* p.31

instance his IP address"[31]. There are few legal frameworks which could allow the use of Sweetie as an investigation method in the criminal investigation, as long as its application stays within the boundaries established by the law. As Sweetie is designed to identify and engage suspects in a manner comparable to undercover investigators, the rules regulating the latter will be decisive for its application. Further, the chatbot will collect certain information on the alleged offender and its devices, and store the content of the communications between that person and Sweetie for investigation purposes. Consequently, the rules authorising these different investigative powers would conjointly be applicable in the case of the chatbot[32].

4. EVALUATION OF SWEETIE ACCORDING TO DUTCH CRIMINAL LAW. NEW DUTCH LEGISLATIVE FRAMEWORK

Following the Report on Sweetie in 2016, Bart Schermer, associate professor at the Centre for Digital Technology and Law at Leiden University, explained the conclusions the team of researchers had reached: "According to Dutch criminal law the use of (virtual) children to lure is not yet explicitly allowed and it is unclear whether webcam sex with a virtual person is punishable anyway"[33] and that had to do with the type of legal system in the Netherlands. "We have a strong action-orientated criminal justice: you have to have committed all the elements that constitute an offense. Because in every sexual offense the victim has to be "a person who has not attained the age of eighteen years", otherwise the offense can never be committed. Sweetie is not a real person."[34]

It was nothing but an opportunity for adopting new legislation in Netherlands. On 21 September 2018, the Computer Crime Act III (*Wet Computercriminaliteit III*) was published in the Dutch Government Gazette and entered into force on 1st of March 2019. The Act managed to improve the Ducth criminal substantial and procedural legislation by amending Dutch Criminal Code (DCC) and the Dutch Code of Criminal Procedure (DCCP). The Act constituted a response to the rapid developments of technology, the internet and cybercrime, following the principles and directions set out in 1993 by the Computer Crime Act I and consolidated in 2006 by the Computer Crime Act II.

---

31 *Ibid.,* p. 48

32 *Ibid.*

33 Terre des Hommes, *Dutch criminal law too limited to use Sweetie*, 20/10/2016, [https://www.terredes-hommes.nl/en/news/dutch-criminal-law-too-limited-use-sweetie], accessed 13. April 2020

34 *Ibid.*

The Computer Crime Act III enables courts and the police to access computers covertly and remotely to investigate serious crimes like child pornography, drug trafficking and targeted shootings. This power extends to personal computers, mobile phones and servers. In addition, the Act gives investigating officers the power to apply various investigative tactics, such as making certain data inaccessible, copying files and tapping communication channels. This will make it more difficult for criminals to use the internet to avoid detection.

Other provisions allow investigating officers to use "decoy teens" in order to facilitate the identification and prosecution of "groomers" who approach minors online for sexual purposes.[35]

One of the most controversial provisions refers to the so-called "hacking power" (provided by Sections 126nba, 126uba 126zpa DCCP). The law enforcement agents are empowered with a new competency: they have the power to access computer systems remotely by stealth under specific conditions. Thus designated investigative officials can access remotely and by stealth a computerized system (computer, smartphone or a server) in use by a suspect. They will hack the system by breaking or circumventing the system's security or by applying software and technical tools.

Since any implementation of the hacking instrument constitutes a severe violation of the privacy of the individual concerned, the Dutch legislator made it possible under restrictive conditions (urgent investigation interest, a warrant from an investigative judge, the suspected offence must constitute a serious breach of legal order and for which the law prescribes a sentence of imprisonment of eight years or more, etc.).

Any data that can be registered may be copied for evidence purposes in a criminal investigation and therefore, the Dutch legislator has established an additional safeguard: the requirement of "logging" (recording data) during the investigation (Section 126ee DCCrP). However, the logged information will not be added (automatically) in the case-file, the defense must expressly request for it.

Among other amendments stands the extended criminalization of the offence of "grooming"[36] (Sections 248a and 248e DCC). Until the new Act entered into force, the law enforcement authorities had to use decoy victims, essentially police

---

35 [https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime], accessed 13. April 2020

36 The term "grooming" is used to denote the unwanted practice of soliciting minors over the internet with the objective of sexual abuse

officers impersonating minors under the age of 16 (because caselaw established that a suspect of grooming could not be punished if the victim, pursuant to the previous Section 248e DCC, was identified as a person not having reached the age of 16). Under the Computer Crime Act III, Sections 248a and 248e DCC were amended to ensure that the offence also related to soliciting, for sexual purposes, any person "impersonating an individual not having yet reached the age of 16 or 18".[37]

Some of the amendment brought by the Computer Crime Act III could make possible the use of Sweetie in the criminal investigation phase, allowing Dutch law enforcement agents to reach an effective result in their fight against online pedophilia.

5. EU COUNCIL TACKLES NATIONAL LEGISLATORS

EU Council has adopted recommendations pressuring the national legislators to think outside the box and[38] reiterated the importance of timely action to investigate and prosecute offenders and rescue child victims of sexual abuse and exploitation from situations of ongoing harm. The national competent authorities were invited to make the widest possible use of the existing tools and mechanisms available at national and EU level, in particular at Europol and Eurojust. The Council highlighted the necessity of having appropriate and specific tools in order to fight against online child abuse, including the possibility for the competent authorities to exploit the data collected during investigations. To this end, the Council recalled its conclusions of the JHA Council of 6 and 7 June 2019, underlining that data retention is essential for effective investigation and prosecution of serious crimes. Furthermore, legislative reforms should maintain the legal possibility for schemes for retention of data, in accordance with the principles laid down in the EU Charter of Fundamental Rights.

In this regard, the Council encouraged Member States to develop and apply innovative investigation methods as well as consider allocating specialized law enforcement resources to combat child abuse and sexual exploitation. The exchange of good practices among Member States adds value to these initiatives.

---

37 Nosh van der Voort, David Schreuders, *Pioneering Dutch Computer Crime Act III entered into force*, 01 March 2019, [https://www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force], accessed 13. April 2020

38 Council of European Union, *Conclusions on combating the sexual abuse of children* – Council conclusions 12862/19, 8 October 2019, Paragraphs 10-15, [https://data.consilium.europa.eu/doc/document/ST-12862-2019-INIT/en/pdf], accessed 13. April 2020

The Council considers industry, and in particular online platforms, to be a key contributor to preventing and eradicating child sexual abuse and exploitation, including the swift removal of child sexual abuse material online. Notwithstanding current efforts, the Council notes that more must be done to counter technical, legal and human challenges that hamper the effective work of competent authorities.

Given the exponential increase in child sexual abuse material online, the Council urges the industry, including online service providers, to ensure lawful access to digital evidence for law enforcement and other competent authorities. The Council invites online service providers to remove or disable access to contents identified as child sexual abuse material online as soon as possible after becoming aware of such content. It calls on the Commission to propose measures to address this growing challenge.

A global, coordinated approach to fight this type of crime is important, including cooperation with third countries and other key stakeholders.

6. INTERESTING NATIONAL CASELAW OF EU COUNTRIES

At the end of December 2019, Eurojust had published another Issue of the Cybercrime Judicial Monitor, pointing out some of interesting national caselaw which raised the question of using Artificial Intelligence tools in the criminal process. [39]

On 14 December 2018, the Court of Appeal of Amsterdam convicted the defendant to the maximum penalty of 10 years and 243 days imprisonment for, among other offences, possession, production, distribution of child sexual abuse material, (attempt to) sexually abuse children, computer intrusion and possession of software for this purpose, extortion and swindling, following a previous conviction decided by the Court of First Instance in Amsterdam.

In 2013, following the receipt by the Dutch police of two reports from Facebook, a criminal investigation was started. According to Facebook, an unknown person with at least 86 interconnected Facebook accounts was collecting, producing and distributing images of child exploitation. This unknown person also blackmailed dozens of underage girls, using the images in question. He also blackmailed a number of adult men. He recorded images on which these men masturbated while they assumed that they were in contact via the webcam with underage boys. He

[39] Eurojust, Cybercrime Judicial Monitor, Issue 5 December 2019, p. 10-12, [http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/cybercrimejudicialmonitor/CJM%20Issue%205%20-%20December%202019/2019-12_CJM-5_EN.pdf], accessed 13. April 2020

subsequently demanded money to be paid, threatening to distribute the images among the friends and family of the men. According to Facebook, false identity credentials, protected IP addresses, protected Internet connections and a Dutch IP address were used. During the investigation, the suspect's telephone number and house address were found. With the authorization of the judge, a keylogger[40] was placed on two computers in the suspect's house, and microphones were placed to record confidential communications. The suspect was arrested at home in 2014 and many of his goods were seized, including a laptop, a desktop and a large number of hard disks. Digital investigation has shown that a number of these data carriers contained many files that can be linked to the facts.

The defendant argued that the results of the keylogger installed on the laptop and desktop computer in the defendant's home, with which screenshots and keystrokes have been recorded, cannot be used for evidence purposes because (a) the keylogger was used unlawfully, and (b) the accuracy of the keylogger's results is in doubt.

The advocate-general opposed both points, stating that the inspection of the keylogger before its installation was both possible and sufficient. Furthermore, the irregularities with regard to the keylogger did not affect the reliability of the results. Secondly, with regard to the absence of the keylogger on the defendant's computer after his arrest, the Court reasoned that the user of the computer himself has likely disabled or deleted unwanted software from his computer, including the keylogger. With regard to the recording by the keylogger of other (non-confidential) communication, the Court stated that this additional recording could be regarded as an unavoidable side-effect of the recording of screenshots. However, this situation does not justify the conclusion that the keylogger has not been used in a normal way or that an irregularity has occurred.

The Court further examined whether the defendant actually used the accounts and the extent of the network of accounts. The offences of which the defendant was charged were committed on the Internet. Given the fact that the accounts refer to each other, it seemed that the accounts were used by one person and that they belong together.

---

[40] A keylogger (short for keystroke logger) is software that tracks or logs the keys struck on the keyboard, typically in a covert manner so that the person using the computer doesn't know that his/her actions are being monitored. Keyloggers can be used to intercept passwords and other confidential information entered via the keyboard. As a result, the person who installed the keylogger can get PIN codes and account numbers for financial accounts, passwords to someone's email and social networking accounts and then use this information to various purposes, in trhis case to discover the perpetrator's identity and the criminal acts he/she committed. See McAfee, *What is a keylogger?*, 23 July 2013, [https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger/] accessed 05. June 2020

In regard with one of the accusations, the defendant argued that, since the contact with the victim was via webcam, no physical contact took place and no form of force was placed on the victim. This force must be of such an extent that the victim had no other option than to cooperate, according with Dutch legislation. As the victim gave no sign of resistance, this force was not an issue, thus no attempt to sexual assault had taken place. The Court reasoned that the rationale behind Article 246 Criminal Code means that 'forcing a person to commit an act by means of threat of fact can only exist if the suspect, by means of the threat of that fact, has deliberately caused the victim to have committed those acts against her will'. The fact that the defendant deliberately put pressure on the victim, threatening to distribute nude pictures of her to friends and family, clearly showed that the victim felt forced to commit the sexual acts.

Another interesting case was that of Mathiew Brown King Bell, in 2019.[41] For the first time, a person was convicted of live-streaming the sexual abuse of children. The police relied almost entirely on the evidence of the offences that the accused had recorded. In addition, the identities of the victims are still unknown. Moreover, issues were encountered during the investigation, involving the transmission of intelligence from Terres des Hommes to the National Crime Agency in the UK and delay in them passing that intelligence on to Police Scotland. During this period, the accused continued to offend.

In this case, the accused was involved in the live-streaming of sexual abuse in the Philippines while residing in his home in Scotland. He was paying less than EUR 1 for each abuse to be committed. The offences of which he was convicted include conspiracy to rape and sexual offences against children.

The accused pled guilty, so no trial took place and no judicial consideration was made of the charges used to prosecute. The judge in sentencing did explicitly state that he was sentencing as though the accused had committed the offences in person. The UK domestic sexual offences law was tested to see if such behavior committed while live-streaming could be prosecuted. As with previous online sexual offences, this test has been successful without any extensive discussion by the Court.

7. CONCLUDING REMARKS

The criminal investigation faces new times that bring a lot of challenges: the professionalization of criminals, especially in the field of crimes committed online,

[41] *HMA v Matthew Brown King Bell* 2019, [http://www.scotland-judiciary.org.uk/8/2235/HMA-v-Matthew-Brown-King-Bell], accessed 13. April 2020

the proliferation of criminal phenomenon gathering new features such as technology and transnational component or the Internet offering environment. These challenges force investigators and other judicial bodies to adapt and be creative in their fight against crime. Artificial Intelligence and all its applications might be the key to successfully enforce the criminal law but using such novel tools could challenge the legislative framework of the states. Despite the opening and inventiveness of AI designers and programmers, their good intentions and noble goals, futuristic investigative tools cannot be used during the investigation faze in the absence of a very solid legal framework. The use of such tools may put human rights and due process standards at risk, so they require extreme caution.

The inventive tools, such as chatbots, allow investigators, as we have seen, to capture a criminal even before he/she commits the crime. However, from a legal point of view, this "efficiency" is actually the weak point of the use of such tools. In the contemporary law system, crimes can only be conceived by reference to a human perpetrator and a human victim, in compliance with the principle of legality: an act cannot be sanctioned by criminal law unless it is provided, as a consumed form or as an attempt by law. Or, as we have shown, in Sweetie's case, there is neither a human victim nor a crime (not even in the form of an attempt), essential conditions for a repressive criminal intervention.

The only solution for using a chatbot to catch criminals is a legislative intervention in the sense of introducing among the criminal procedural provisions new methods of supervision or criminal investigation on the one hand, and, on the other hand, the introduction of special norms in the criminal law providing that, in the situation of committing the deed against a virtual victim, this particular act would be assimilated to an attempt and sanctioned as such. Only in this way the standards of a fair trial could be met. The implementation of the EU Council's recommendations on the development and application of innovative investigative methods cannot lead to breaches of the principle of legality or the standard of a fair trial, no matter how effective the outcome of these efforts in the fight against crime is. One thing is certain: criminal and criminal procedural legislation must keep pace with the digitalization of crime and must adapt to new forms of crime, otherwise the legal instruments of reaction will be completely ineffective.

We place ourselves in favor of innovative approaches of the crime phenomenon but with respect of legal principles and fundamental human rights. The future will show us if the appeal to AI instruments was a good choice…

REFERENCES

BOOKS AND ARTICLES

1. Baarfield W.; Blitz, M.J., *Research Handbook on the Law of Virtual and Augumented Reality*, Edward Elgar publishing, 2018
2. Jackson A.R.W.; Jackson J.M., *Forensic Science,* second edition, Pearson, 2008
3. Nissan, E., *Computer Applications for Handling Legal Evidence, Police Investigation and Case Argumentation*, *vol*. 1, Springer, 2012, p. 767-836
4. Schermer, B. W. *et al., Legal Aspects of Sweetie 2.0*. Leiden/Tilburg: TILT, 2016

EU LAW

1. Council of European Union, *Conclusions on combating the sexual abuse of children* − Council conclusions 12862/19, 8 October 2019

WEBSITE REFERENCES

1. [https://www.ibm.com/security/intelligence-analysis/i2/law-enforcement], accessed 13. April 2020
2. Açar, K.V., *Webcam Child Prostitution: An Exploration of Current and Futuristic Methods of Detection*, International Journal of Cyber Criminology, January – June 2017, *vol*. 11, no. 1, pp. 98–109, [DOI: 10.5281/zenodo.495775], accessed 13. April 2020
3. Bex, F. *et al., Sense-making software for crime investigation: how to combine stories and arguments?*, Law, Probability and Risk, *vol*. 6, issue 1-4, March 2007, pp. 145–168, [https://doi.org/10.1093/lpr/mgm007], accessed 13. April 2020
4. Crawford, A., *Computer-generated ‚Sweetie' catches online predators*, BBC News, 5 November 2013, [https://www.bbc.com/news/uk-24818769], accessed 13. April 2020
5. Crăciun V., *Ce este un chatbot?* ["What is a chatbot?"], Today Software Magazine, Nr. 72, 2018, [https://www.todaysoftmag.ro/article/2645/ce-este-un-chatbot], accessed 15. April 2020
6. Hare, J., *What is metadata and why is it as important as data itself?* Opendatasoft, 25 August 2016, [https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data], accessed 15 April 2020
7. *HMA v Matthew Brown King Bell* 2019, [http://www.scotland-judiciary.org.uk/8/2235/HMA-v-Matthew-Brown-King-Bell], accessed 13 April 2020
8. Kidd, C., *Chatbot vs Virtual Agent: What's The Difference?,* BMC Blogs, 27 November 2019, [https://www.bmc.com/blogs/chatbot-vs-virtual-agent/], accessed 5 June 2020
9. Schweizer, K., *Avatar Sweetie exposes sex predators*, The Age, April 26, 2014, [https://www.theage.com.au/world/avatar-sweetie-exposes-sex-predators-20140425-379kf.html], accessed 13. April 2020
10. *Sweetie* at [https://youtu.be/aGmKmVvCzkw?t=10], accessed 13 April 2020

11. Terre des Hommes, *Dutch criminal law too limited to use Sweetie*, 20/10/2016, [https://www.terredeshommes.nl/en/news/dutch-criminal-law-too-limited-use-sweetie], accessed 13. April 2020
12. Terre des Hommes, *First conviction for child abuse in Belgium thanks to Sweetie*, 9/04/2015, [https://www.terredeshommes.nl/en/news/first-conviction-child-abuse-belgium-thanks-sweetie], accessed 13. April 2020
13. Tiffany Lam, How immersive technologies (AR/VR) will reform the human experience, TEDxQueensU, on [https://www.youtube.com/watch?v=Fi97-DAcGMk], accessed 15. April 2020
14. Van der Voort, N.; Schreuders, D., *Pioneering Dutch Computer Crime Act III entered into force*, 01 March 2019, [https://www.simmons-simmons.com/en/publications/ck0bi70lg7kew0b94qi4inld1/280219-pioneering-dutch-computer-crime-act-iii-entered-into-force], accessed 13. April 2020
15. Varshney, U. *et al., Voice over IP*, Communications of the ACM, *vol.* 45, no. 1, 2002,pp. 89-96, [https://dl.acm.org/doi/10.1145/502269.502271], accessed 15. April 2020
16. McAfee, *What is a keylogger?*, 23 July 2013, [https://www.mcafee.com/blogs/consumer/family-safety/what-is-a-keylogger/], accessed 5 June 2020
17. [https://www.government.nl/latest/news/2019/02/28/new-law-to-help-fight-computer-crime], accessed 13. April 2020.
18. Eurojust, Cybercrime Judicial Monitor, Issue 5 December 2019, [http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/cybercrimejudicialmonitor/CJM%20Issue%205%20-%20December%202019/2019-12_CJM-5_EN.pdf], accessed 13. April 2020
19. [http://www.holmes2.com/holmes2/index.php], accessed 13. April 2020
20. [https://www.savesweetienow.org], aaccessed 13. April 2020
21. [www.terredeshommes.nl], accessed 15. April 2020