Consultation on the White Paper on Artificial Intelligence – A European Approach – Victim Support Europe

Victim Support Europe (VSE) welcomes the EU consultation on the White Paper on Artificial Intelligence. As the leading European umbrella organisation advocating on behalf of all victims of crime, no matter what the crime, no matter who the victim is, VSE has been representing interests of all victims of all crimes since its foundation. VSE represents around 60 national member organisations, providing support and information services to more than 2 million people affected by crime every year in 30 countries. We work towards this mission through advocacy to improve EU and international laws, through research and knowledge development and through capacity building at the national and local level.

As a starting point, in our view, it is critical that the EU takes into account in its AI related activities, the opportunities that AI presents to improve the situation of victims and to assist in the fight against crime, as well as the dangers it poses in particular in the way that criminals may use AI to support their criminal activities. AI applications should be designed in such a way that it can't be used to facilitate crime – or at least in a way to minimise such risks, and options to use AI applications to support civil society and overcome or reduce the effects of crime should be developed. The following paragraphs will elaborate on VSE's stance on the three sections mentioned in the survey accompanying the White Paper.

Section 1 – An ecosystem of excellence

VSE believes that partnership with the private sector in the development of AI is very important. However, civil society should be included in this process in order to make sure that victims' issues and fundamental rights are taken into account with the development of such applications. It is a fundamental flaw in the EU's innovation, research and legislative action if civil society actors are not seen both as potential beneficiaries of AI but also as contributors to the design of the technology. Not only is this true of civil society, but also the public sector, which must be supported in its adoption and use of the technology. AI applications have already been successfully implemented in the form of street policing and the detection of online fraud and more opportunities should be explored to fight crime and also improve the treatment of victims.

Additionally, we support increases in financing for start-ups innovating in AI. Funding in this area should not, however, exclude participation of civil society. Indeed, funding programmes should support the inclusion of civil society organisations as well as priorities relevant to civil society activities such as supporting victims of crime. The proposed action of setting up a public-private partnership for industrial research is very important but seems to exclude civil society.

Section 2 – An ecosystem of trust

As for building an ecosystem of trust, VSE thinks it is important to understand the risks of AI. AI may endanger safety, as it may be used to facilitate certain crimes like phishing. AI systems can enhance attackers' efficiencies and generate thousands of new email addresses to be used for phishing in a matter of seconds. Additionally, AI generated voices (such as Google Duplex) could be used to scam

people over the phone. These situations may make it more difficult for persons having suffered harm to obtain compensation. If a crime is committed by or with the help of an AI system, who is to blame? Recovering damages could be an impossible task. Of course, it is almost impossible to make a crime proof system. The EU must therefore be proactive in ensuring that the public are made aware of new risks and emerging crimes, that they understand how to protect themselves and that sufficient laws, policies and practices are in place to help people in the event that they do become victims.

In addition to crime based risks, is that the use of AI may lead to discriminatory outcomes. VSE recognises the risks that AI may result in discriminatory results or breaches to fundamental rights. As a rights based organisation, we strongly support any EU action aimed at eliminating or reducing such risks.

The concerns expressed above can and should be addressed by applicable EU legislation or appropriate non-legislative action. Current legislation on AI may have some gaps, as it is unclear whether EU legislation sufficiently addresses these issues and further research and consultation should be carried out to determine if there is sufficient legislative protection in place with respect to the use of AI for criminal purposes.

Whilst we support compulsory requirements on high risk applications in order to limit any risks, and we understand the need to balance crime mitigation with economic feasibility, we believe that compulsory requirements should not just be limited to high-risk applications. For example, tracking apps meant for parents to track what their children are doing on their smartphones may be used by perpetrators of domestic violence or stalkers to track their victims' online activities.

There are several uses of AI that are concerning from a victim's perspective. We already mentioned AI being used in phishing attacks, where the system can generate a human-like voice or create realistic email addresses. Additionally, AI systems can use machine learning to analyse companies' websites and use their brand voice to create more realistic phishing emails. Criminals will use AI to carry out more and better phishing attacks, create increasingly powerful self-spreading malware, weaken authentication controls, and cheat rule-based transaction monitoring. The only way to prevent this from happening is to incorporate safety by design, making sure that a new AI application can't be used for criminal purposes or at least that such applications have strong safeguards in place. Importantly, 'safety and accessibility by design' should be a fundamental principle; AI applications need to be safe and accessible, regardless of its user. Any possible risk needs to be assessed in the development stage of a new AI application and law enforcement and the private sector need to be assisted in creating countermeasures and investigative tools in lockstep with the development of the AI applications. Too often, enforcement is playing catch up to new technologies taken on by criminals.

Section 3 – Safety and liability implications of AI, IoT and robotics

An important risk that needs to be expanded on to provide more legal certainty, is the use of AI to facilitate the undermining of democratic values. As we mentioned earlier, AI could be used to tamper with elections or spread fake news. This means that AI has the potential to become a threat to democracy.

Despite the wide array of risks mentioned above, AI can also be useful to support civil society and reduce the effects of crime. For example, AI can play a big role in resiliency training for victims of crime. Additionally, AI and big data can provide new statistics on (likelihood of) victimisation and help policy makers write better public policies. VSE therefore encourages active consideration of how such risks and benefits can be addressed.