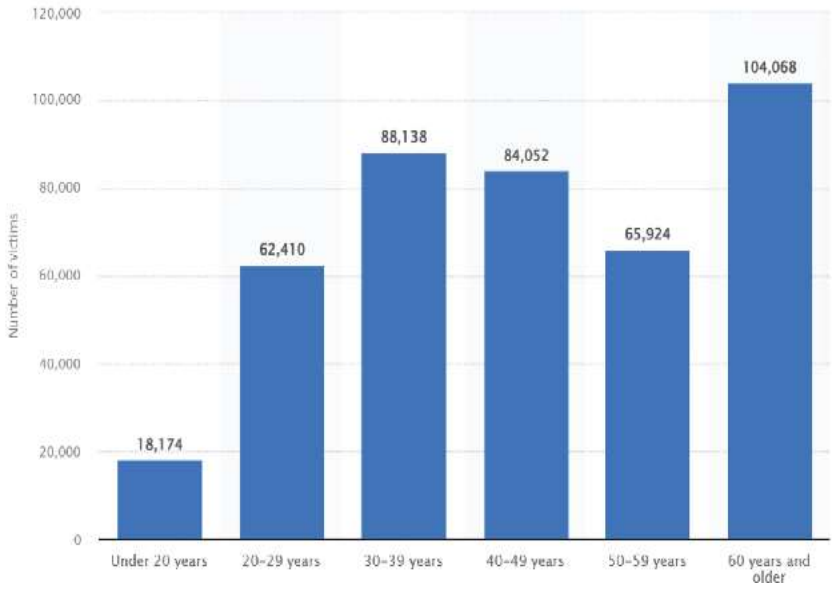
How Can Political Institutions Protect Older Persons from Criminal Activities?

HEINZ KURT BECKER

First of all, let me express my gratitude to the NGO Committee on Ageing, UN Vienna, for holding this side event and the opportunity to make a contribution to the topic of the digital abuse of the elder generation.
Having experience as former Member of the European Parliament and Vice President of the European Seniors' Union, I understand that besides the priorities on social, health and care matters, the challenges caused by the rapidly developing digital technologies are the most relevant for seniors nowadays and in the future.

Digital revolution brought a lot of benefits for seniors such as internet, smart phones and other means of connection to the world. But it hides also some risks such as criminal actions against unaware seniors. To provide tools for protection, we might organize trainings for users of elder generations to ensure safe living with and in the digital world. This leads us directly to the topic of elders' abuse and cybercrime, such as fraud as the most frequent type of crimes against the elderly.
The vulnerability of many elderly people has made them a target for criminals in the worldwide web. There are some statistics illustrating the grade of digital abuse as a form of cybercrime against elder generation. Statistics taken from the United States, year 2023 is considered to be the most representative as it comes from the country, which is one of the most digitally developed.

Number of cyber crime victims in the United States in 2023, by age group[1]



The data show the following:

Cybercrime victims in the 60 plus pop-

[1] *Source: Statista, U.S cyber crime victims 2023, by age, published by Ani Petrosyan, Apr 3, 2024, URL: https://www.statista.com/statistics/1390164/us-victims-cyber-crime-by-age/*

ulation are nearly double than in the 20 to 29 years age group.

Cybercrime against the elderly is on the rise worldwide. The main reason is that more and more seniors are getting active online, especially since the pandemic, and the trend is increasing even further.

Prime reasons why older adults are often more vulnerable to financial exploitation and online fraud are their limited knowledge about the functioning of the internet, insufficient digital literacy and a lack of familiarity with online threats and also a (kind of) trusting nature.

Loneliness and isolation some seniors live in, very often makes them seek social connections online, making them more vulnerable to scammers, pretending to offer friendship or emotional support. It happens because seniors may not always be able to read correctly the intent behind messages. They get exposed to the risk of falling victim to social engineering attacks, which can result in financial loss or misuse of personal information. In addition, older persons are more vulnerable to identity theft because they are often more trusting and can therefore be easily exploited financially by fraudsters. Older persons often have built up savings through a lifetime of work and/or investment and may therefore do not consequently monitor their credit and financial accounts.

Understanding the urgency of the problems and challenges, legal regulations, such as the Digital Services Act (DSA) of the European Union has addressed these irritating and damaging phenomena. The Digital Services Act focused on user security, the protection of fundamental rights, the prevention of illegal or harmful online activities as well as the spread of disinformation. While preserving a fair, safe and freely available Internet environment. Such legal provisions is what our elderly population is expecting.

The *Digital Services Act* of the EU is somehow a logical follow up of two other legal regulations of the EU:

The EU's General Data Protection Regulation, in force since 2018, (according to which, for example, the Facebook parent company Meta had to pay a fine of 1.2 billion euros in Ireland - the reason for this is an incorrect procedure when passing on data from Europe to the USA) and the Copyright Directive, in force since 2019, (here, 6 states have already been sued for non-implementation and - corporations like YouTube as a whole have accepted and implemented the upload filters, according to which music, images, written works or video recordings can no longer be used without asking or without payment).

Now, the new Digital Services Act (DSA) is the next step of the EU in regulating the digital world. The organisations and companies regulated by the DSA include all globally leading online platforms such as marketplaces (largest is Amazon), social networks (most popular are Facebook, WhatsApp, Instagram, etc.), content sharing platforms (no.1 is YouTube), app stores (dominant are Apple, Samsung, etc.) as well as travel and

accommodation portals (like Booking.com). The risk of illegal content is widely spread on popular online platforms and search engines.

Therefore, the DSA makes platforms reaching more than 10% of Europe's consumers a subject to specific rules which are important because of the specific risks. Large-scale internet services may carry harmful elements with illegal content and destructive impact to fundamental rights, public safety and welfare affecting European individuals and the society as a whole.

For example, these large size companies are obliged:

- to establish a contact point for authorities and users;
- to report crimes on their platforms;
- to offer user-friendly terms and conditions;
- to guarantee transparency regarding advertising, recommendation systems or content moderation decisions.

They must proactively identify, analyse and assess systemic risks associated with their services in cases of:

- illegal content;
- fundamental rights such as freedom of expression, media freedom and media pluralism, discrimination, consumer protection and children's rights;
- public security and electoral processes;
- gender-based violence, public health, child protection and mental and physical well-being.

The big players on the internet:

- are subjected to an inspection once a year;
- must send their user data to the European Union, forwarded to the Commission and the national authorities for control;
- and must provide verified "Artificial Intelligence (AI) experts" with access to their platform data to enable the detection and identification of systemic risks to EU citizens.

Since February 2024, the new rules apply to all platforms - to the so-called very large online platforms and online search engines, which I mentioned before, already since the end of August 2023.

And the penalties are very painful: Fines of up to 1% of global annual turnover can be imposed by the EU - for Google with around 200 billion euros turnover, a fine of 2 billion euros – that would hurt anyone.

The *Digital Service Act* (DSA) also regulates what most people are interested in – these are the artificial texts, photos, videos, etc. which can be easily created by Artificial Intelligence (AI) and provide people with false content, distort the truth, enable financial fraud and even influence elections.

At the top of the *Digital Service Act* is the regulation that Artificial Intelligence (AI) MUST always be clearly marked. Users must be able to immediately recognize when a certain content

was generated by using AI. Synthetic audio, video, text and image content must be labelled and recognized as artificially created or manipulated - subject to high penalties for non-compliance.

Considering the effects of the rapid digital revolution, the elder generations and all of us are faced we must put the next resulting question:

How can we help elder citizens be more protected?

The fact that 75% of internet users in the EU have bought something online at least once. Therefore, it is a must to look for best possible protection for elder people.

Above all, it is important to strengthen the digital skills of senior citizens as broadly and deeply as possible and make everyone use the new technologies in a responsible and safe manner - through education and training, from childhood on and of course in their professional life up to the old ages. Lifetime learning must be the rule.

This requires major initiatives by governments at national and regional level, as well as by local authorities and the social partners, which must live up to their respective responsibilities.

Measures can be financial assistance programs supporting civil society associations and private initiatives in the organisation of courses for elder citizens to acquire digital knowledge and competence. This could be accompanied by my favourite model, even if it sounds a bit trivial: Communities and/or civil society organisations may establish intergenerational groups, where young volunteers educate elders in acting in the digital world and learning about the dangers and risks of online communications. The young people should be thoroughly prepared for this task, which may need only a few hours' workshop. To summarize: Despite all the problems we are dealing with today, I want to end with a positive statement: Whatever challenges will come, let's not be afraid, we will master – because if we act now,

"The future can be better than its present reputation!"