European Commission

OPINION OF THE SUB-GROUP ON ARTIFICIAL INTELLIGENCE (AI), CONNECTED PRODUCTS AND OTHER NEW CHALLENGES IN PRODUCT SAFETY TO THE CONSUMER SAFETY NETWORK

[*December – 2020*]

Justice
And Consumers

EUROPEAN COMMISSION

Directorate-General for Justice and Consumers
Directorate E — Consumers
Unit E4— Product safety and Rapid Alert System

European Commission
B-1049 Brussels

OPINION OF THE SUB-GROUP ON ARTIFICIAL INTELLIGENCE (AI), CONNECTED PRODUCTS AND OTHER NEW CHALLENGES IN PRODUCT SAFETY TO THE CONSUMER SAFETY NETWORK

• INTRODUCTION

In 2005, the Consumer Safety Network (CSN) was set up as an informal group of experts, in order to stimulate reflection and discuss topics related to the safety consumer products and to provide a knowledge base for the related policy work. The Commission services responsible for product safety can set up sub-groups to the CSN to address specific issues. The Commission's Directorate General for Justice and Consumers (DG JUST) set up a Sub-group on artificial intelligence (AI), connected products and other new challenges on product safety in December 2019.

The sub-group was tasked with assessing whether and to what extent the existing EU framework for product safety is adapted to emerging new technologies (connected products, Artificial Intelligence[1]– - etc.). In particular, it was asked to assist the Commission in developing an assessment on the need for adaptations of the Directive 2001/95/EC on general product safety (GPSD) in this regard. This assessment takes into account sectorial/harmonisation product legislation and relevant ongoing reviews of this legislation[2].

• CHALLENGES TO THE CONCEPT OF SAFETY

Article 2(b) of the General Product Safety Directive provides the following definition of a safe product:

'safe product' shall mean any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, taking into account the following points in particular:

- *(i) the characteristics of the product, including its composition, packaging, instructions for assembly and, where applicable, for installation and maintenance;*
- *(ii) the effect on other products, where it is reasonably foreseeable that it will be used with other products;*
- *(iii) the presentation of the product, the labelling, any warnings and instructions for its use and disposal and any other indication or information regarding the product;*
- *(iv) the categories of consumers at risk when using the product, in particular children and the elderly.*

The feasibility of obtaining higher levels of safety or the availability of other products presenting a lesser degree of risk shall not constitute grounds for considering a product to be 'dangerous'.

[1] As defined by the High-Level Expert Group on Artificial Intelligence in April 2019: *Artificial intelligence systems are software (and possibly also hardware) systems designed by humans that, given a complex goal, act in the physical or digital dimension by perceiving their environment through data acquisition, interpreting the collected structured or unstructured data, reasoning on the knowledge, or processing the information, derived from this data and deciding the best action(s) to take to achieve the given goal. AI systems can either use symbolic rules or learn a numeric model, and they can also adapt their behaviour by analysing how the environment is affected by their previous actions.*

[2] According of Article 1.2, the General Product Safety Directive applies insofar there are no more specific provisions with the same objective in other pieces of Union legislation.

This legal definition can be understood as addressing many types of risks by which a product can, directly or indirectly, cause harm to consumers[3]. However, it can be claimed that traditionally the definition has been interpreted as exclusively applicable to risks that have a physical impact on the safety of persons, among others mechanical or chemical risks.

The following sections summarise the information concerning new elements of products in the era of AI and connectivity, and highlight the new risks.

New elements arising from AI, Interconnectivity, and Human-Product Interaction

Currently, some products in the EU market present the following characteristics:

- They do not only contain software but also interact with software located in the Cloud (e.g. IoT platform) or with software installed on third-party smart devices (e.g. applications installed on smartphones or tablets).
- They are connected to the Internet and/or to other products.
- They can be used to access services.
- They can be used to process and collect personal and non-personal (meta)data.
- Their software consists partly of adaptive algorithms[4] and their software can be updated remotely after their placing on the market.
- They allow a higher degree of human-product interaction.

New risks

Cybersafety

As described above, two common characteristics of new technology products are the fact that they are connected and the potential evolution of their software. This entails that products may be vulnerable to hacking and other cyber-attacks. Beyond the criminal responsibilities of the malicious party, cybersecurity can also have an impact on the safety features of the product (it can be denominated as "cybersafety"): for instance, when a connected product lacking cybersecurity features is hacked and as a result can harm the safety and health of consumers. A notification submitted by Germany via the Rapid Alert System for dangerous non-food products in 2015 regarding a passenger vehicle illustrates this[5]. Cars were recalled because the radio in the vehicle may have had certain software security gaps allowing unauthorised third party access to the interconnected control systems in the vehicle. If a hacker exploited these software security gaps for malicious purposes, a road accident could have occurred.

[3] Relevant progress has been carried out and is ongoing with respect to the special needs of persons with disabilities (e.g. adoption of the European Accessibility Act Directive (EU) 2019/882 and related standardisation work, new Consumer Agenda).

[4] The lack of a proper handover / disengagement procedure when the AI's prediction is unreliable may result is dangerous situations. Particular risks may arise with so-called "self learning" algorithms that will seek to adapt to the consumer, if such adaptation leads to exploration of responses that affect the consumer's safety.

[5]Notification from Germany on the EU Safety Gate (A12/1671/15) of a passenger car. Available at: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12/1671/15&lng=en

Personal security risks

An additional issue is that new technologies can also pose risks not only because they can have a direct impact on the health and safety of the consumers, but also because through connectivity, they can be indirectly used as a tool to put at risk their personal security. For example, in 2019 the Icelandic authorities notified to the Commission via the Rapid Alert System for dangerous non-food products the recall of a smart watch for children presenting personal security risks[6]. The Icelandic authorities stated that the product itself would not cause a direct harm to a child wearing it, but as the mobile application of the product lacked a minimum level of security, it could be easily used to have access to a child and potentially cause harm. This was especially relevant as the product's main function was to keep the child safe.

Beyond the safety of the device's user, a compromised or hacked device can present a threat to others through cyberattacks being launched through the device. This has become an issue given the rapidly increasing number of connected devices, which may lack cybersecurity features.

However, it is unclear under which legal or policy instrument such personal security risks should be tackled so that consumers are effectively protected against such threats.

Mental health risks

This section points out several issues in relation with new technologies. It needs to be noted that some of these issues do not originate from new technologies. They were prevalent before the digitalisation of the society and continue to be widespread in the off-line world today.

- **Digital feedback systems and the negative psychological effects of user performance rankings:** Some consumers may draw psychological benefits from competition-oriented direct feedback and the online "ranking" of their contributions, while others will be put off significantly by such feed-back, may even perceive it as a form of "harassment", become stressed, depressed, or even suicidal as a consequence of diminished self-esteem. Quite clearly, the manner in which individuals are led to interact with a computer-controlled system in a given context can have negative short and long-term effects on their well-being and overall behaviour, including online behaviours[7]..
- **Connected technologies and the negative effects of multitasking on cognitive ability:** There is evidence that multitasking may be linked to poorer performance in a number of cognitive ability tests[8]. It appears therefore relevant to inform users and consumers of the risks of multitasking and about their selective information processing capacities and, ultimately, their good judgment of what matters most in incoming information streams, on social media and other online platforms, and to educate the public towards using online media parsimoniously and critically.
- **Connected products as a cause of depression, loss of sleep, altered brain function and myopia or early blindness in children and affecting adults greatly:**

[6] Notification from Iceland on the EU Safety Gate Website: A12/0157/19. Available at: https://ec.europa.eu/consumers/consumers_safety/safety_products/rapex/alerts/?event=viewProduct&reference=A12%2F0157%2F19&lng=en

[7] Cheshire, Antin, 2008. Journal of Computer-Mediated Communication, 13: 705–727.

[8] Uncapher, Wagner, 2018. Minds and brains of media multitaskers: Current findings and future directions. Proceedings of the National Academy of Science USA, 115(40): 988

The use of connected devices and smartphones has increased rapidly in recent years. Symptoms such as depression, anxiety, and poor sleep quality may be associated with smartphone overuse in student[9]. and other populations[10] Public measures and public awareness campaigns could be implemented that may help mitigate these risks. In addition, parents and educational institutions should be prompted towards limiting the time for online activity by children and teenagers to a minimum.

- **Virtual reality applications:** There is evidence that virtual simulations of three-dimensional space can measurably affect the precision of human motor behaviours[10]. Another identified challenge with virtual reality applications is that of virtual "doppelgangers"[11] in videogames and other applications. Doppelganger games were found to have measurable effects on an individual's cognitive ability, with memory loss and loss of control over their personal identity, in the game and potentially beyond[12].

Having said that, it can be argued that EU product safety legislation and in particular the GPSD relates to risks arising intrinsically from the design of the product. Risks to mental health that are not intrinsic to the product, but come from the use of a product in particular ways (eg. if a product is used to view content supplied by third parties, some of which could cause emotional distress, or if a product contains communication tools that are used to interact with other people that could lead to, for example, bullying), should not be considered part of the concept of "safety" in the GPSD. It can be therefore argued that these non-intrinsic risks should be dealt with in other policy areas, as in practice it would be difficult or impossible for a manufacturer to assure safety from these risks when designing a product and placing it on the market.

• CHALLENGES TO THE CONCEPT OF PRODUCT

According to Article 2(a) of the General Product Safety Directive, *'product' shall mean any product — including in the context of providing a service — which is intended for consumers or likely, under reasonably foreseeable conditions, to be used by consumers even if not intended for them, and is supplied or made available, whether for consideration or not, in the course of a commercial activity, and whether new, used or reconditioned.*

Software

The Directive does not explicitly include the term 'software' and as such does not explicitly include or exclude software from the definition of the concept of product.

Software is associated to products in different ways and also can be used to access services. In order to find the right answers and suitable solutions under the GPSD, the Subgroup believes it useful to distinguish between four scenarios involving software: (i) embedded software

[9] K. Demirci, M. Akgönül, A. Akpinar, 2015. Relationship of smartphone use severity with sleep quality, depression, and anxiety in university students. Journal of Behavioral Addictions, 4(2): 85–92.

[10] Dresp-Langley B. Children's Health in the Digital Age. Int J Environ Res Public Health. 2020 May 6;17(9):3240. doi: 10.3390/ijerph17093240. PMID: 32384728; PMCID: PMC7246471.

https://pubmed.ncbi.nlm.nih.gov/32384728/

[10] A. Batmaz, M. de Mathelin, B. Dresp-Langley, 2017. Seeing virtual while acting real: Visual display and strategy effects on the time and precision of eye-hand coordination. PLoS One,12 (8): e0183789.

[11] Virtual representations that may look like a person but act independently

[12] J.N. Bailenson, K.Y. Segovia, 2010. Virtual Doppelgangers: Psychological Effects of Avatars Who Ignore Their Owners, In W.S. Bainbridge (ed.), Online Worlds: Convergence of the Real and the Virtual, Human-Computer Interaction Series. Springer: London.

contained in / installed on the product;, (ii) software to be designed/installed on the product, (iii) software interacting with the product but not contained in / installed on the product (e.g. software in the Cloud or software installed on third-party smart devices); (iv) stand-alone software.

Despite the current version of the GPSD is in theory broad enough to cover safety risks resulting from software. , it appears important to clarify the scope of the Directive, to close any remaining gap and to evaluate in which way risks caused by software linked to a product could be mitigated.

- **CHALLENGES TO THE CONCEPT OF PLACING ON THE MARKET AND WHO BEARS THE RESPONSIBILITY**

One of the main requirements of the GPSD is that producers must place only safe products on the market. Implicitly, the safety of the product is assessed at the time that it is placed on the market, i.e. the moment of the first making available of the product in question.

As already said above, one of the common characteristics of AI and IoT products is the presence of software that can change / evolve over time. This challenges the traditional meaning of the concept of placing on the market – which is a crucial element of the safety and liability concepts under EU law.

The technological developments on connected consumer products call for a new framing of the safety obligations that a producer of a connected product needs to comply with. The product that is placed on the market is inherently designed in such a way as the software that is associated with the product will be regularly updated and potentially upgraded.

This design needs to go hand in hand with a move from the static concept of safety at the time of first commercialisation of a product, to the concept of *continued safety*: at the time of the design the producer of a connected product has to build its safety taking into account the probability of subsequent modifications to this product including the modifications that might be brought to its safe functioning linked to software modifications.

In other words, **a connected product must be safe over its whole expected lifespan**.

Who is responsible for safety

It is the producer of the connected product who has the obligation to design that product initially in such a way that it remains safe during its whole expected lifespan, taking into account the (non-substantial) modifications that will or might be brought to this product. The safety documents to be provided by the producer needs to indicate the steps undertaken to protect the safety of the product against risks linked to future modifications of that product.

If the producer introduces substantial modifications to the product in the course of its lifespan, this can be considered as a new placing on the market and the producer should, where appropriate, update their assessment of the safety of the product and any related documentation.

In case substantial modifications affecting the safety of the product are brought to the connected product by a third party, this is to be considered as a new placing on the market by

that party. In this situation, the economic operator who introduces such substantial modifications is considered to be the new producer of that product.

What is a 'substantial modification'?

Depending on whether a modification is substantial or not, new obligations can arise as to how the producer must ensure that the product is safe. How can economic operators be advised on whether the modifications that they wish to introduce are substantial?

- The question arises whether the provisions already existing in the GPSD are sufficient to cover this question : indeed Article 2(b) of the GPSD says that : *(b) "safe product" shall mean any product which, under normal or reasonably foreseeable conditions of use including duration and, where applicable, putting into service, installation and maintenance requirements, does not present any risk or only the minimum risks compatible with the product's use, considered to be acceptable and consistent with a high level of protection for the safety and health of persons, (...).* Consequently, any modification that would not match this definition would be considered as a substantial modification.
- Another approach,[13]:, would be that a modification is deemed to be substantial if the 3 following criteria are cumulatively present:
    - The modification changes the intended functions, type or performance of the product[14].
    - The nature of the hazard has changed or the level of risk has increased because of the modification.
    - The modified product is made available. (This criterion would not apply if consumers has made the substantial modification themselves.)

Please note that the current GPSD refers to the notion of reconditioning of products, and considers as manufacturer of a reconditioned product the person who reconditions that product.

It must be noted that if it is demonstrated that the consumer introduces at their own initiative a substantial modification into the product, the initial producer is not considered to be in charge of the safety obligations related to that modified product, as such a substantial modification by the consumer would not comply with the concept of "foreseeable conditions of use" that is included in the GPSD.

Maintenance and repair

Maintenance and repair operations by third parties are not considered to be substantial modifications. This being said, a product that has been substantially modified by a third party repairer should be considered as a new product. There is a new placing on the market and the third party repairer is the producer.

It is important in this context to provide a clear regulatory framework so that the safety obligations for the producers are rolled out in a way that is compatible with the right to repair of

[13] This approach is currently being discussed in the context of the Radio Equipment Directive 2014/53/EU Preliminary Q&As on certain issues arising in relation to the security of products (connected products) as well as software) or in the draft revised Blue Guide from July 2020

[14] To note that the party introducing the substantial modification will need to take into account the foreseeable use as established in the GPSD.

the consumers, as well as the right to access by independent providers maintenance or repair services.

In other words, it is key that the safety procedures set by the producer when designing the product do not lead to an automatic functional stop of that product or of its connected functions, where a "non-authorised" party engages in maintenance or repair. This also leads to the issue of the accessibility of codes by third parties for maintenance or repair reasons.

• RECOMMENDATIONS FROM THE SUBGROUP

Based on the points above, the Sub-Group acknowledges that a renewed definition on the concept of 'safe product' of the GPSD is needed, and that this would need to be complemented with other actions.

Recommendations related to the GPSD

The Subgroup:

1. Recommends that the Commission update the legal definition of 'safe product' of the GPSD in view of the following elements;
    a. To make an explicit reference to cybersecurity risks that can have an impact on product safety (cybersafety).
    b. To clarify, that if mental health[15] harm is intrinsically caused by a product itself, that should be addressed by the revised GPSD; at the same time asks the Commission to carry out further research in this area;
    c. To reflect that in the safety assessment, several aspects that could have an impact on safety should be taken into account, namely the evolving, learning and predictive functionalities of a product, and the impact of interconnected products.
2. Recommends that the Commission carry out a consistency check of EU legislation concerning personal security risks so consumers are effectively protected against such threats.
3. Recommends that the Commission update the definition of 'product' of the GPSD making explicit in the legal definition and its recitals that it can include possible safety risks related to software interacting with the product;
4. Recommends that the Commission clarify in the GPSD revision that products should be safe over their whole expected lifespan;
5. Recommends that the Commission explore the introduction of the concept of 'substantial modification' and makes third parties which make substantial modifications to a product responsible for the safety of that product instead of the original producer;
6. Asks the Commission to ensure legal consistency within the provisions of the GPSD as well as between complementary legislations in the field of consumer product safety and related fields (GPSD, PLD, Machinery Directive, RED, LVD, Toy Safety Directive, cybersecurity legislation, Digital Services Act, new horizontal instrument on AI, Sales of Goods Directive, the Digital Content Directive, upcoming initiatives under the Chemicals Strategy, etc.), in order to avoid grey zones, overlaps and loopholes;

[15] The WHO definition of health already refers to mental health https://www.who.int/about/who-we-are/frequently-asked-questions

7. While acknowledging the challenge of defining the prescribed level of cybersafety, recommends that the Commission consider to adopt, in addition to the revision of the GPSD, harmonised minimum cybersecurity market access requirements supplemented by European harmonised standards.
8. Recommends awareness raising on the fact that producers of connected products must pay particular attention to the links between product safety, the protection of personal data and privacy of the users of those products.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696, or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications from: https://op.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.