Position Paper

Euralarm Response to EC call for evidence on Digital Networks Act – 8 July 2025

Introduction

Euralarm takes the opportunity of the call for evidence issued by the European Commission on a Digital Networks Act to raise an issue faced by our members with the phasing out of mobile technologies. The present Position Paper follows our briefing on "risks and challenges of uncoordinated shutdown of 2G and 3G networks" responding to the EC's White Paper "How to master Europe's digital infrastructure" and the discussion Euralarm had in February 2025 with DG-CNECT on this topic. It explains the issue, provides references highlighting it and proposes some elements for incorporation in the future Digital Networks Act. The proposal is also in line with Priority 3 (Empowering end-users) of BEREC's draft Strategy 2026-2030 where they call for a close monitoring of the process for phasing out legacy networks to prevent negative impacts.

Impacts of phasing out of 2G and 3G networks on electronic Fire safety and Security services

Most of the intruder and hold-up alarm systems and fire detection systems across Europe are equipped with a transceiver sending the alarms, fault messages and audio and video streams (e.g. for alarm verification) to an alarm receiving centre or a response authority. These transceivers rely generally on the mobile communication networks for delivering their messages. The hardware of those transceivers is specific to the mobile technology that is accessible and affordable at the time of development of the product.

Communication networks change and are updated to new technologies. On one hand, new generation arises almost every 10 years and their life-cycle are becoming shorter. On the other hand, security and safety systems have a very long life (up to 20/25 years) which doesn't match with the shorter lifetime of the mobile generations. While such systems are key for the security and safety of people, households and small business, there is a complete lack of visibility and of coordination between the telco operators and the safety and security systems providers (and the rest of the IoT industry) in this regard. Telecom operators may not have a clear view on the amplitude of the issue because neither the end-users of the safety and security systems nor the service companies installing and maintaining those systems are direct customers of them. Such systems are usually equipped with roaming SIM cards that are not emitted by a particular operator and can be used wherever in Europe (standardised product manufacturing).

Migration from a technology to another one may take more than 7 years: 3 years at least for device design, testing, certification and manufacturing + 4 years of operational migration (material cost of the migration, visit to customer premises, complex migration as it involves cooperation from end user).

Publications from both private and public entities highlight the same issue:

- In 2023 BEREC published the **"Report on the outcome of the public consultation"** on the draft "Report on practices and challenges of the phasing out of 2G and 3G"[1], in which it concludes that, in the face of a

[1] https://www.berec.europa.eu/en/document-categories/berec/reports/summary-report-on-the-outcome-of-the-public-consultation-on-the-draft-report-on-practices-and-challenges-of-the-phasing-out-of-2g-and-3g

shutdown of 2G/3G technologies, operators must consider minimization of negative impacts on the user and provide greater transparency in shutdown plans.

- This same recommendation has been included in the EC **White Paper "Building Europe's digital infrastructure of tomorrow: towards a Digital Networks Act"[2],** which includes the need to coordinate the switching off of these technologies, as well as the continuity of services that are being provided on them.
- In December 2023, the **Finnish Ministry of Communications** approved **a change in the conditions of operators' licenses** so that the 2G band would have to be **maintained until 2029[3].**
- In June 2024, **PWC** published "**Impact evaluation of 2G/3G shutdown in France**", focusing on 5 types of devices with high social impact. Conclusions show that: (1) Replacing 2G/3G equipment is complex and can take **4–10 years, depending on the sector**. (2) The shutdown **has increased costs and delayed innovation**. (3) **Critical services are at risk**: over 50,000 life-threatening teleassistance calls could be missed/year; 12 million residents in lifts may be affected; 970,000 people and small businesses could lose alarm protection; 500,000 sleep apnea patients may face health risks; and 2,000 emergency eCalls could go unanswered each year.
- In France, the Parliamentary Higher Commission for Digital Technology and Postal Services has issued a **report demanding stricter regulations for 2G and 3G networks switch-off**, to ensure that the stakeholders concerned will not be penalized. It mentions the lack of communication and preparation between actors about the shutdown of 2G/3G and concluded about the possible shutdown of 4G/5G[4].
- Norwegian Parliament decided to conduct an **impact assessment of the shutdown of the 2G-network in March 2025**[5]. Consultation was conducted by the **National Communications Authority (Nkom)** until May 15th, with the goal of identifying businesses and suppliers that have or provide services related to security and emergency, and that have not yet planned for the transition to 4G and 5G. As final goal Nkom wants to develop a **realistic mapping and impact assessment** to prevent users of critical societal systems and equipment from being surprised when 2G technology is no longer available. Nkom aims to deliver this assessment before August 2025.

Regulatory proposals

There is a need to promote harmonisation and coordination in the future network migration and evolution.

The new Digital Networks Act (DNA) should make clear that the current European Electrocommunications Code (EECC) Article 45 can be used by Member States to intervene and clarify possibilities of Member States to intervene in the network shutdown plans. More specifically, the DNA should:

1. establish obligations for Telco providers to communicate to each national Regulator its plan for networks transition and the specific dates for shutdown;
2. provide for obligation for Telco providers to keep Regulators updated of any potential news regarding its shutdown plans and deadlines;
3. allow Regulators to intervene or even veto those shutdown plans if services continuity is not granted.

The DNA should include that any change on communication networks that might impact continuity of end-users' services shall ensure end users' rights by the following measures:

1. public consultation to identify all actors impacted and difficulties and obstacles posed by the network changes;
2. 7 years of minimum notice to ensure visibility to end-user;

[2] White Paper "Building Europe's digital infrastructure of tomorrow: towards a Digital Networks Act"
[3] https://lvm.fi/en/-/changing-licence-terms-for-telecom-operators-2g-technology-to-be-maintained-until-end-of-2029
[4] Avis-n°2025-02-du-10-avril-2025-sur-les-consequences-de-la-fin-des-technologies-2G-et-3G.pdf
[5] https://nkom.no/fysiske-nett-og-infrastruktur/informasjon-om-slukking-av-2g-i-2025#generell_informasjon_om_slukkingen_av_2gnettene

3. information campaign to ensure that all stakeholders are fully informed;
4. ensure continuity of emergency and essential services;
5. help vulnerable populations maintain access to the services.

Finally, the DNA should ensure that at least one operator with national roaming guarantees coverage for a sufficient period of time, even if the rest of the operators begin the shutdown process.

Conclusion

Technological changes on networks must be coordinated between regulators, end-users and network providers as network connectivity is a key element to ensure products and services performance. A visibility and notice period of 7 years should be given to manufacturers and operators to adapt strategies and operations.

The present paper provides some proposals for incorporation in the DNA and we are available for further discussing them.

About Euralarm

Euralarm represents the fire safety and security industry, providing leadership and expertise for industry, market, policy makers and standards bodies. Our members make society safer and secure through systems and services for fire detection and extinguishing, intrusion detection, access control, video monitoring, alarm transmission and alarm receiving centres. Founded in 1970, Euralarm represents over 5000 companies within the fire safety and security industry valued at 67 billion Euros. Euralarm members are national associations and individual companies from across Europe.

Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

DISCLAIMER

Note: The English version of this document, TC-A-0262, is the approved Euralarm reference document.