FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

ENCRYPTION AND CONCERNS ABOUT ACCESS TO PRIVATE ONLINE COMMUNICATION

PEOPLE'S VIEWS ACROSS THE EU

REPORT

Contents

O tej publikacji 3

Key findings 4

Introduction 5

1. Concerns over access by various actors to private information communicated online 7

Results 7

2. Views on the importance of encryption to protect private online communication 14

Results 14

Ways forward 18

Endnotes 19

O tej publikacji

© European Union Agency for Fundamental Rights, 2026

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the European Union Agency for Fundamental Rights copyright, permission must be sought directly from the copyright holders.

Neither the European Union Agency for Fundamental Rights nor any person acting on behalf of the Agency is responsible for the use that might be made of the following information.

Luxembourg: Publications Office of the European Union, 2026

HTML

- TK-01-26-018-EN-Q
- ISBN: 978-92-9489-809-8
- DOI: 10.2811/4263124

PDF

- TK-01-26-018-EN-N
- ISBN: 978-92-9489-810-4
- DOI: 10.2811/2763158

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS Rennweg 12 – 1030 Vienna – Austria

Contact FRA

- Website
- LinkedIn
- Instagram
- Facebook
- YouTube
- X

Key findings

A significant share of people in the EU are concerned about information from their private online communication being accessed without their knowledge or permission – such as when using WhatsApp, Signal, iMessage or other private messaging applications/direct messaging:

- *62 % are concerned about their private communication being accessed by criminals.*
- *Almost half of the people in the EU are concerned about access to their private communication by foreign governments (49 %) or businesses (47%).*
- *Some two in five (ranging from 37 to 42 %) people are concerned about access by law enforcement, their national government, or their country's secret or intelligence services.*
- *The degree of concern varies significantly among Member States. For example, concern over access by law enforcement without people's knowledge or permission ranges from 11 % to 58 %.*

Three in four people (77 %) in the EU view the use of encryption to protect one's private online communication as very or fairly important:

- *45 % consider the use of encryption as very important. By comparison, only 12 % do not consider it as important.*
- *Encryption is considered as important by the majority of people in all EU Member States. However, the share of people who see it as important varies among Member States, from 53 % to 89 %.*
- *The importance attached to encryption is higher among those who expressed concern about various actors accessing their private online communications without their knowledge or permission, as well as among people who use the internet frequently.*

Introduction

As our lives increasingly move online, use of online channels for private communication has become an everyday feature. In this context, encryption of electronic devices and communication is a standard tool. It serves as a key privacy enhancing technology as well as a cybersecurity guarantee, recognised also in EU law and policy instruments [1]. Human rights bodies [2] have underlined the vital role of encryption as an enabler of human rights. Besides the fundamental right to respect for private and family life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union ('Charter'), preserving confidentiality of communications also contributes to safeguarding other rights such as the protection of personal data (Article 8 Charter) or freedom of expression and information (Article 11 Charter).

At the same time, use of encrypted devices or communication by criminals has been repeatedly highlighted as a growing challenge for law enforcement, as encryption can make it difficult to access digital data needed for criminal investigations. Following the *ProtectEU* Internal Security Strategy [3] issued in 2025, the European Commission is preparing a Technology Roadmap on encryption, to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner in the context of investigations, while safeguarding cybersecurity and fundamental rights.

This short paper contributes to these discussions. It presents data on how concerned people are in the EU about various actors accessing their private information which is communicated online, as well as the importance that people attach to encryption to protect such communication.

The findings are based on an EU-wide Eurobarometer survey of 26,453 respondents, with specific questions developed by FRA. For more detail on the methodology and data collection, see About the data collection. Separately, FRA is also planning to release findings from its ongoing qualitative research on the fundamental rights implications – in practice – of accessing digital data for criminal investigations, which involves in-depth interviews with practitioners from law enforcement, prosecution and judicial authorities, as well as defence lawyers, service providers and legal and technical experts.

About the data collection

The data presented in this document are based on the Eurobarometer survey wave 104.2. Data collection was carried out between 6 and 30 November 2025 by the survey company Verian Belgium. The questions that FRA developed for the Eurobarometer survey were included among other survey modules. The use of the Eurobarometer is coordinated by European Commission's Directorate-General for Communication, 'Public Opinion & Citizen Engagement' Unit.

FRA joined the data collection by adding and financing the inclusion of specific

questions related to views about and experiences with online services. This included online fraud, hate speech and content moderation, child safety, as well as privacy and data protection.

This paper briefly presents results relating to questions addressing people's views on the use and importance of encryption to protect private online communication.

The survey covers people living in the 27 European Union Member States, aged 15 years and over. The 26,453 respondents were randomly selected and results weighted to match the demographic profile in each country by gender and age, urbanisation and region. The data are representative of the population in each Member State and of the European Union.

1. Concerns over access by various actors to private information communicated online

In the survey, respondents were asked to indicate how concerned they are about the possibility of various actors having access to information they communicate privately online. The question asked in the survey was as follows:

- *'How concerned are you that some of the information you share in private online communication (such as when using WhatsApp, Signal, iMessage or other private messaging applications/direct messaging) might be accessed by any of the following without your knowledge or permission?'*

The respondents were asked to consider in turn each of the six actors listed in Figure 1 and indicate their answers on a scale from 1 to 7, where 1 means 'not at all concerned' to 7 means 'extremely concerned' (for details on the scale and its use see the note under (Figure 1).

FRA's separate Fundamental Rights Survey – which collected data in 2019 from 34,948 respondents – examined the degree to which people in the EU are concerned about various actors accessing information they have shared on the internet, including on social media, when this access takes place without people's knowledge or permission. The results – which have been analysed in FRA's Fundamental Rights Report 2020 [4] and in the 2020 paper, *Your rights matter: Data protection and privacy* [5] – show that most internet users (55 %) are concerned about their information being used without their knowledge or permission by one or more actors listed in the survey (such as criminals, businesses and advertisers, law enforcement agencies or intelligence services, (prospective) employers, and foreign governments).

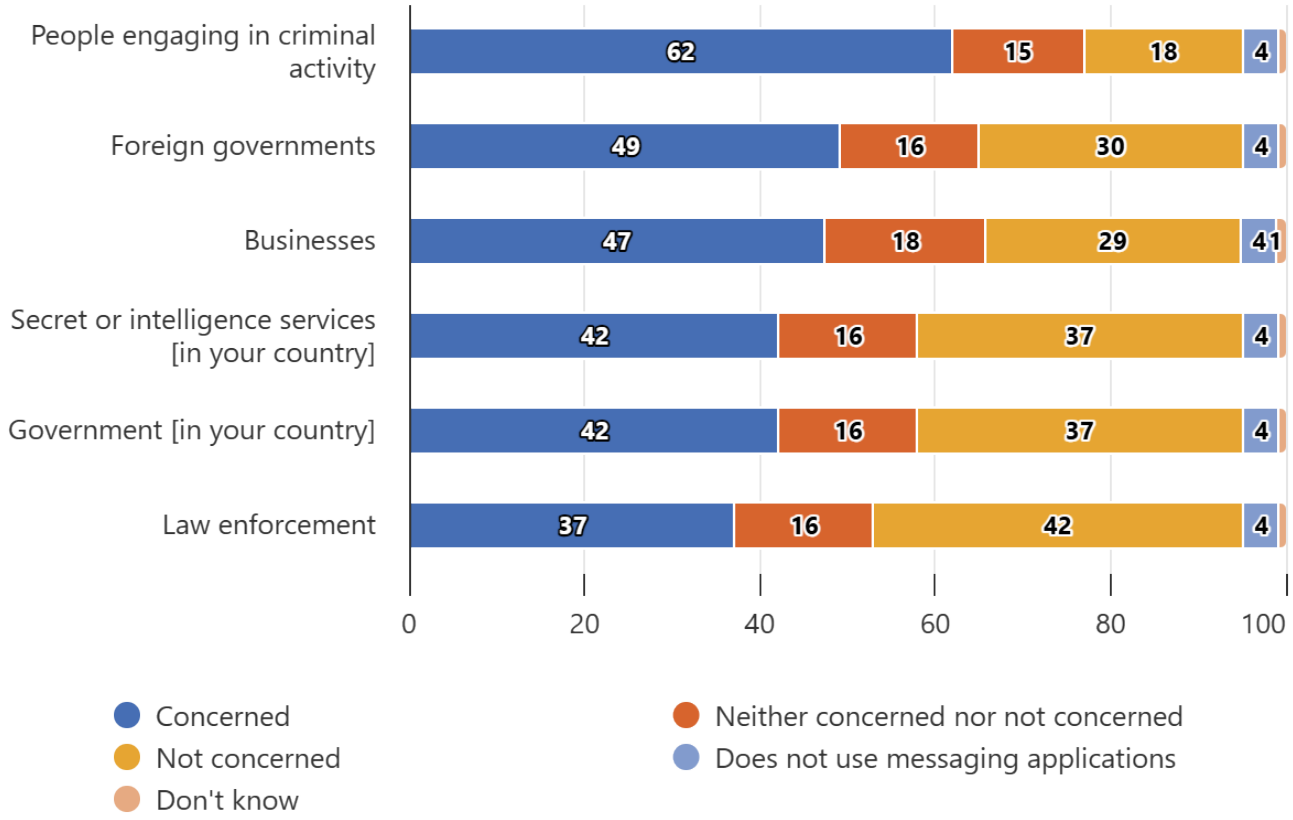
Compared with the question asked in the Fundamental Rights Survey, the current survey focuses specifically on information shared via private online communication, and the list of potential actors involved is partly different (for the actors listed in the current survey, see Figure 1). However, while not directly comparable, both surveys indicate heightened concern when it comes to access – by certain groups – to people's online communication.

Results

The majority of people in the EU, 62 %, are concerned about information from their private online communication being accessed by criminals (Figure 1). Almost half of people in the EU are concerned about access to their private online communication by foreign governments (49 %) and businesses (47 %). Some two in five people are concerned about access to their private online communication by national secret or intelligence services (42 %), national governments (42 %), and law enforcement (37 %). Overall, three in four people (75 %) are concerned about access to their private online communication *by at least one* of the six actors listed in Figure 1. In the the

survey, respondents were asked to indicate for each of the six actors in Figure 1 the degree of concern they had about each actor accessing one's private online communications without a respondent's knowledge or permission.

Figure 1 – Concerns over selected actors accessing one's private online communications without their knowledge or permission (EU-27, %)



The stacked bar chart shows the levels of concern of respondents regarding access without their knowledge or permission to their private online communication, by different actors. 62 % are concerned about access by people engaging in criminal activity, followed by 49 % about access by foreign governments, 47 % by businesses, 42 % by the respondent's national secret or intelligence services, 42 % by the respondent's national government, and 37 % by law enforcement.

NB: n = 26,453

Question: *'How concerned are you that some of the information you share in private online communication (such as when using WhatsApp, Signal, iMessage or other private messaging applications/direct messaging) might be accessed by any of the following without your knowledge or permission?'*. Respondents were asked to provide an answer with respect to each of the actors listed in the figure above. They were asked to respond using a scale ranging from 1 to 7, where 1 means 'not at all concerned' and 7 means 'extremely concerned' – or that they don't use messaging applications, or to select the answer category 'Don't know'. Above, respondents who answered with a value 1–3 are included in the category 'Not concerned', value 4 is labelled 'Neither concerned nor not concerned', and values 5–7 are shown in the category 'Concerned'.

Source: FRA, 2026

People who use the internet every day/almost every day and those who use it less often express similar rates of concern as each other, ranging from 59 – 65 % of them concerned about access by criminals, to 38 % of them – across both groups – concerned about access by law enforcement.

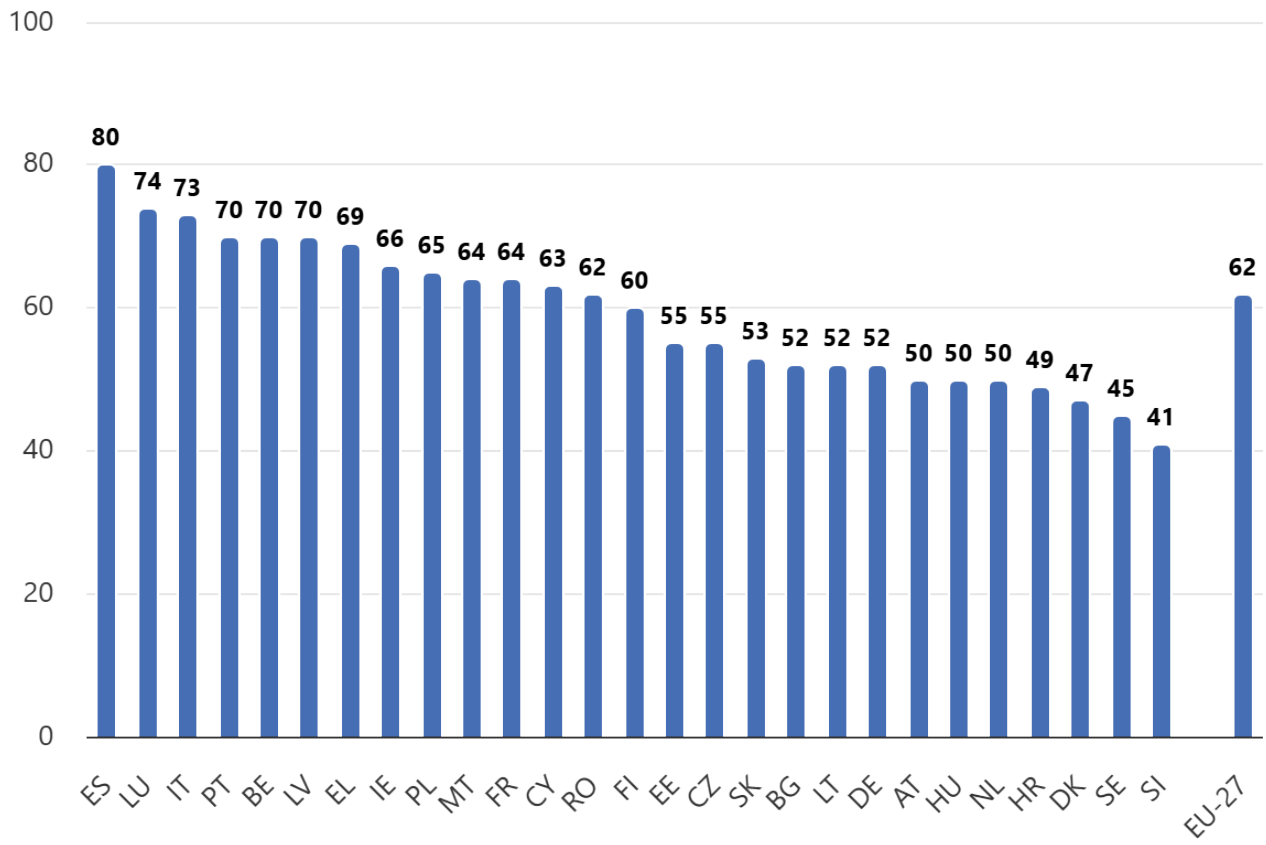
Concern over access by different actors does not differ notably between women and men, with 63 and 62 % of women and men, respectively, being concerned about access by criminals, and 36 to 50 % concerned about other actors, with no more than 2 % points of difference in concern for each actor. In relation to age, people over 55 years old have lower concern regarding all actors. However, the age group 55+ also includes a higher number of people who do not use messaging apps compared to other age groups. When people who do not use messaging apps are removed from the analysis across all age groups, the levels of concern are broadly similar across all age groups.

Similarly, differences between people according to their level of education largely reflect differences in the use of online messaging. When focusing only on respondents who are users of online messaging, levels of concern are closer across educational categories. People in the intermediate category in terms of education (those with upper secondary education or post-secondary but non-tertiary education) express the highest concern, meaning there is no clear pattern of increasing or decreasing concern by people's level of education. For example, regarding access to online communication by foreign governments, 42 % of people in the lowest of the three education categories analysed express concern, compared to 54 % of those in the intermediate education category, and 48 % of those in the highest education category (tertiary education).

Rates of concern about different actors accessing online data differ greatly across EU Member States. In some countries, such as Italy, Malta, Poland, Portugal and Spain, rates of concern are generally high (Table 1), ranging from 63 to 80 % for access by criminals (Figure 2). Regarding other actors, concern in these countries ranges from 44 to 67 %. On the other hand, Denmark, Finland, Lithuania, the Netherlands and Sweden score the lowest, ranging from 41 to 50 % respondents concerned about access by criminals, and 11 to 31 % about access by other actors.

While access by law enforcement is generally associated with lower concern, in 18 Member States, at least one third (33 %) of people express concern about it, with the highest rates in countries such as Cyprus, Italy, Malta, Poland, Romania and Spain (Figure 3).

Figure 2 – Concern over people engaging in criminal activities accessing one's private online communications without user's knowledge or permission, by EU Member State (%)



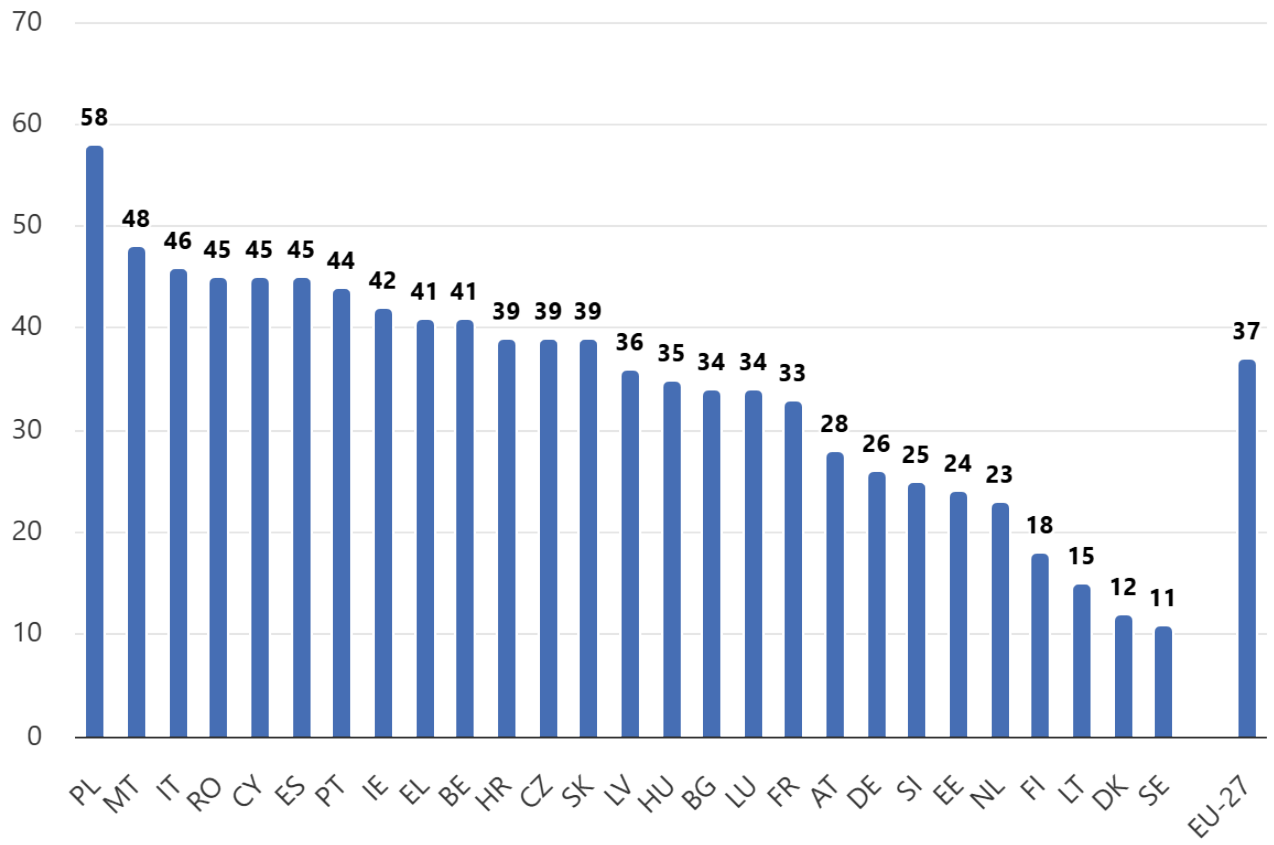
The chart shows the levels of concern of respondents in each EU Member State regarding access without their knowledge or permission to their private online communication, by people engaging in criminal activities. Results range from 80 % of respondents concerned in Spain, to 41 % concerned in Slovenia. The EU average is 62 %.

NB: n = 26,453

Question: For details on the question asked, see notes under Figure 1.

Source: FRA, 2026

Figure 3 – Concern over law enforcement accessing one's private online communications without user's knowledge or permission, by EU Member State (%)



The chart shows the levels of concern of respondents in each EU Member State regarding access without their knowledge or permission to their private online communication, by law enforcement. Results range from 58 % of respondents concerned in Poland, to 11 % concerned in Sweden. The EU average is 37 %.

NB: n = 26,453

Question: For details on the question asked, see notes under Figure 1.

Source: FRA, 2026

Table 1 – Concern over selected actors accessing one's private online communications without their knowledge or permission, by EU Member State (%)

Member States	People engaging in criminal activity	Foreign governments	Businesses	Secret or intelligence services [in your country]	Government [in your country]	Law enforcement
BE	70	56	51	44	46	41
BG	52	30	34	33	31	34
CZ	55	40	34	40	35	39
DK	47	31	30	16	15	12
DE	52	36	33	28	27	26
EE	55	32	31	31	27	24

Member States	People engaging in criminal activity	Foreign governments	Businesses	Secret or intelligence services [in your country]	Government [in your country]	Law enforcement
IE	66	53	52	46	45	42
IT	73	61	55	60	55	46
EL	69	39	48	43	45	41
ES	80	66	67	55	59	45
FR	64	49	50	37	41	33
HR	49	43	43	41	39	39
CY	63	48	50	45	42	45
LV	70	48	48	41	41	36
LT	52	27	24	23	20	15
LU	74	62	64	43	39	34
HU	50	41	35	40	41	35
MT	64	49	44	49	48	48
NL	50	41	41	30	28	23
AT	50	39	34	33	33	28
PL	65	64	60	60	62	58
PT	70	60	57	48	49	44
RO	62	56	53	51	46	45
SI	41	25	27	27	25	25
SK	53	37	31	41	37	39
FI	60	38	40	19	23	18
SE	45	27	32	11	10	11
EU-27	62	49	47	42	42	37

NB: n = 26,453

Question: For details on the question asked, see notes under Figure 1.

Source: FRA, 2026

2. Views on the importance of encryption to protect private online communication

After the question related to unauthorised access to one's private online communication, respondents were asked about their views concerning the importance of encryption to protect one's private online communication.

The question asked in the survey was as follows:

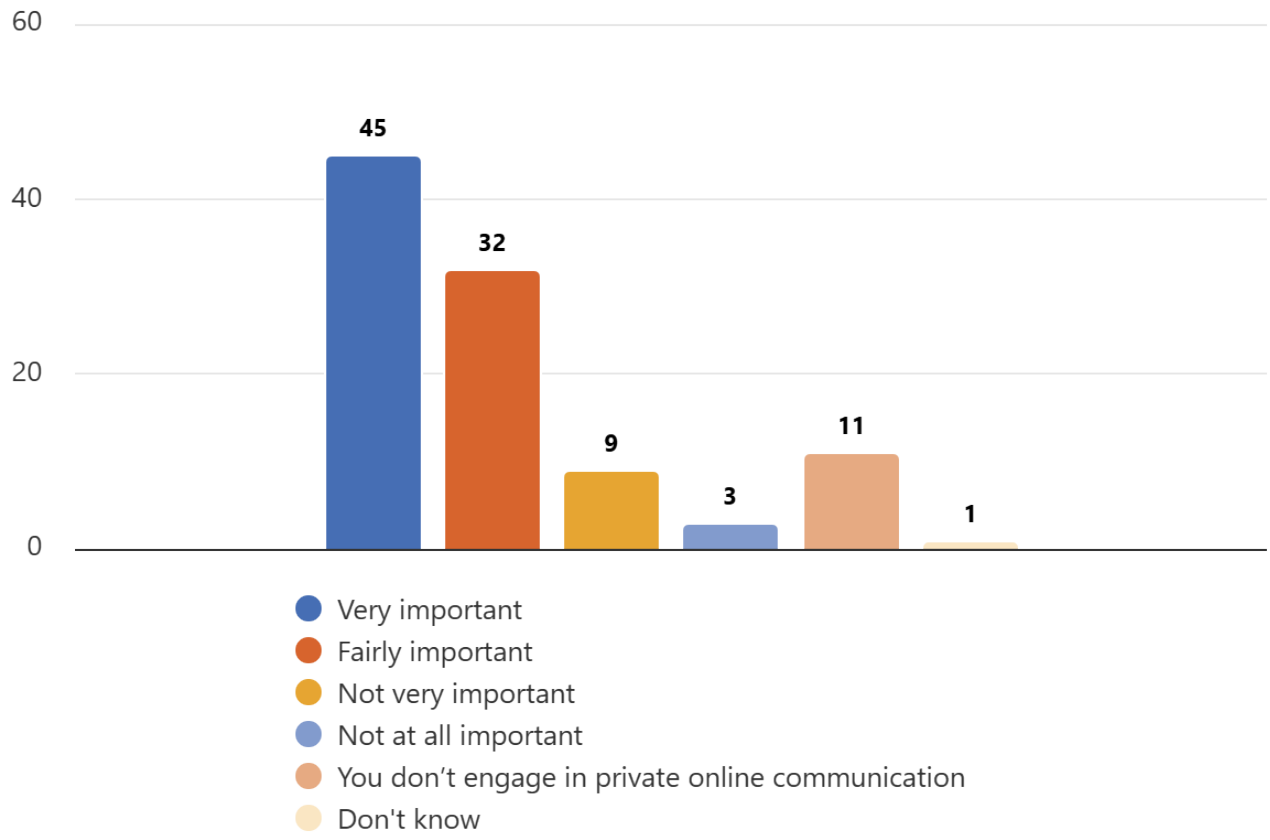
- *'Encryption makes information sent online unreadable to others except the sender and the receiver. How important is it to you that your private communication (such as when using WhatsApp, Signal, iMessage or other private messaging applications/direct messaging) with others is protected through encryption?'*

Respondents could provide their answers on a four-point scale, ranging from 'very important' to 'not at all important', or they could indicate that they don't engage in private online communication.

Results

Three in four people (77 %) in the EU-27 view the use of encryption to protect one's private online communication as very or fairly important (Figure 4). More than two in five (45 %) consider the use of encryption as very important. On the other hand, 12 % of people think it is not very important or not at all important to use encryption to protect a person's private online communication, and 11 % indicate that they do not engage in private online communication.

Figure 4 – Views on the importance of encryption to protect one's private online communication (EU-27, %)



The bar chart shows people's views on the importance of encryption to protect one's private online communication. 45 % see encryption as very important and 32 % as fairly important, while 9 % consider it as not very important and 3 % as not at all important. In addition, 11 % do not engage in private online communication, and 1 % answered 'Don't know'.

NB: n = 26,453

Question: *'How important is it to you that your private communication (such as when using WhatsApp, Signal, iMessage or other private messaging applications/direct messaging) with others is protected through encryption?'* Respondents could answer the question using the categories shown in the figure above.

Source: FRA, 2026

Looking only at people who express concern about various actors accessing their private online communications without permission, 82 % consider it very or fairly important that their private communications are protected by encryption, compared with 63 % among people who are not concerned about various actors accessing their online communication or who give a 'neutral' answer (that is, selected the middle value in the scale from 1 ('not at all concerned') to 7 ('extremely concerned'). Further, 84 % of people who use the internet every day or almost every day view encryption as very or fairly important in protecting their private online communication, as opposed to 61 % who use the internet a few times a week or less often.

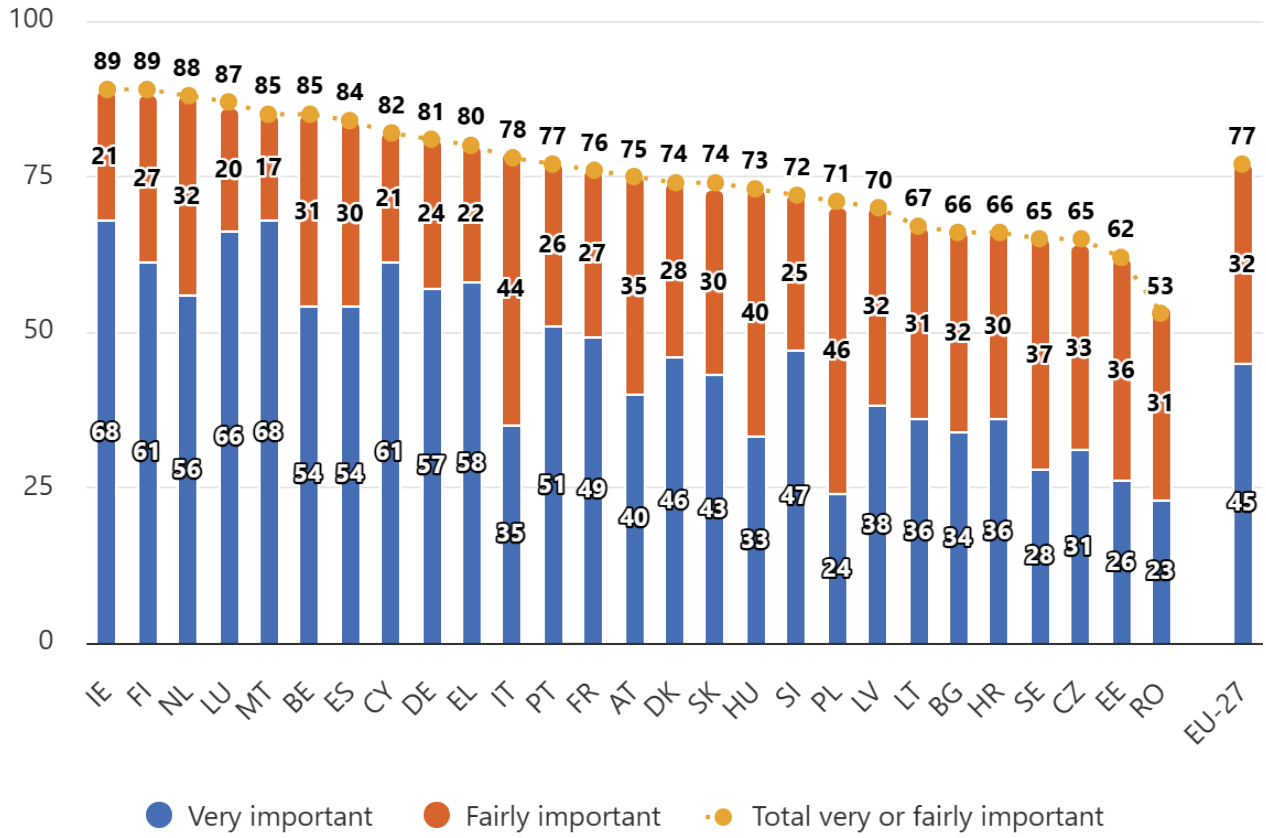
Views regarding the importance of encryption to protect one's private online communication do not differ notably between women and men – 77 % of women and men, respectively, consider it very or fairly important. In terms of age, over four in five people in most age groups consider encryption as very or fairly important, with the exception of people aged 55 years or more. In this age group, 66 % view encryption as very or fairly important – however, the share of people not

engaging in private online communication is also notably higher among people aged 55 and older. If people who don't use private online communication are excluded from the analysis, only minor differences remain between the oldest age group (55+) and others with respect to their views on the importance of using encryption. A similar pattern can be observed with respect to people's education and their views on the importance of protecting private communication with encryption. Differences between those with at most lower secondary education (64 % consider encryption very or fairly important) and those with upper secondary education (79 %) or tertiary education (86 %) to a large extent disappear when people who do not engage in private online communication are excluded.

In all EU Member States, a majority of people view it as very or fairly important to protect one's private online communication with encryption – this ranges from 53 % in Romania, 62 % in Estonia and 65 % in Czechia and Sweden, respectively, to 87 % in Luxembourg, 88 % in the Netherlands, and 89 % in Finland and Ireland, respectively (Figure 5).

The strongest support for the use of encryption – considering it very important – can be found in Malta (68 %), Ireland (68 %), Luxembourg (66 %), and Cyprus and Finland (61 %, respectively).

Figure 5 – Views on the importance of encryption to protect one's private online communication, by EU Member State (%)



The chart shows the views on the importance of encryption according to respondents in each EU Member State. Results range from 89 % of respondents who view it as important in Ireland and Finland, to 53 % of respondents in Romania. Additionally, the chart distinguishes between those who see encryption as very important and those who see it as fairly important. The results range from 68 % in Ireland and Malta, respectively, who see encryption as very important, to 23 % in Romania who see it as very important. The EU average is 77 %, divided in 45 % that see it as

very important, and 32 % that see it as fairly important.

NB: n = 26,453

Question: For details on the question asked, see notes under Figure 4 .

Source: FRA, 2026

Ways forward

By presenting how people in the EU perceive the role of encryption in protecting their private online communication and the degree of concern about various actors accessing their private online information, this paper aims to inform discussions and support policymaking at the EU and Member State levels when deciding on concrete legal and practical measures to facilitate lawful and effective access to data.

In line with the Council conclusions on access to data for effective law enforcement [6] and actions outlined in the *ProtectEU* Internal Security Strategy [7], any measures that will be proposed in this area are to complement existing EU rules that aim to facilitate cross-border access to electronic evidence [8], by introducing tools which would enable law enforcement authorities to access encrypted data in a lawful manner, in full respect of fundamental rights.

FRA will further inform these discussions with the findings from its ongoing research on the use of different encryption workarounds by national authorities during criminal investigations and their impact on fundamental rights in practice, which will be published later this year. [9]

Endnotes

[1] EU Cyber Resilience Act refers to encryption as a means of protecting the confidentiality of stored, transmitted or otherwise processed data, see Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), Annex I, Part 1, 2(e); European Commission's Roadmap for lawful and effective access to data for law enforcement, highlights that encryption and other cybersecurity measures play an important role in protecting information systems from espionage and disruption and securing communications, privacy and personal data. See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Roadmap for lawful and effective access to data for law enforcement, COM/2025/349 final, 24 June 2025.

[2] For example, United Nations, The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/51/17, 4 August 2022; European Data Protection Board and European Data Protection Supervisor, Joint Opinion 04/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, 28 July 2022.

[3] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM/2025/148 final, 1 April 2025.

[4] FRA, Fundamental Rights Report 2020, Publications Office of the European Union, Luxembourg, 2020.

[5] FRA, Your rights matter: Data Protection and privacy – Fundamental Rights Survey, Publications Office of the European Union, Luxembourg, 2020.

[6] Council of the European Union, Conclusions on access to data for effective law enforcement, 16448/24, 12 December 2024.

[7] European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: a European Internal Security Strategy, COM/2025/148 final, 1 April 2025.

[8] European Parliament and Council of the European Union, Regulation (EU) 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings, OJ L 191, 28.7.2023.

[9] For more details, see the description of the research project, Fundamental rights implications of accessing digital data for criminal investigations, on the FRA website.