DIGITAL FOOTPRINT AWARENESS

A study conducted by

www.dlearn.eu

Table of Contents

This report presents the results of the research "Digital Footprint Awareness", a self-sustained survey promoted by the European Digital Learning Network ETS – DLEARN within the DigitEdu 2023 project (Promoting cooperation and research to address the digital needs in the area of education and training in Europe – Year 1). It is a project funded by the European Union under the Erasmus+ programme, Civil Society Cooperation in the fields of Youth, Education and Training.

This survey is designed to collect data on the level of skills the population possesses when it comes to operating online and knowledge of their Digital Footprint.

Over the past few months, we have circulated the online and paper survey both within the DLEARN network and outside, to gather opinions and views on the subject, and we have collected more than 10000 questionnaires from people with different kind of profile and expertiseacross Europe.

This research has allowed us to construct what you will see in the following pages, the level of competences and knowledge of people from all over the EU regarding their digital skills and digital footprint.

The analysis conducted has given us a true cross-section of society in terms of digital skills and knowledge of their digital footprint, and has given us new insights and actions to bridge the gap between what people think they know to be safe online and what they really need to avoid becoming victims of potentially harmful actions against them.

This final report will be shared and discussed with the European Commission, and it is freely available to all on our website[1] and social media.

Executive Summary

Foreword

Gianluca Coppola

President of the European Digital Learning Network ETS

Although the concept of the digital footprint is no longer as new and unknown as it was in 2019, when we conducted our first survey, it is unfortunately still a difficult concept to understand and remember, especially for younger people, such as children and teenagers, as well as for older people who are not as used to technology.

Let's start with a definition: The term DIGITAL FOOTPRINT, also known as digital shadow or electronic footprint, refers to the trace of data left behind when using the Internet, including websites visited, emails sent and information transferred online. A digital footprint can be used to keep track of an individual's online activities and the devices they use. Whether actively or passively, internet users create a digital footprint.

We leave a trail of information, known as a digital footprint, every time we use the Internet. For example, posting content on social media, subscribing to a newsletter, leaving an online review or shopping online increases the size of our digital footprint.

We leave a trail of information, known as a digital footprint, every time we use the Internet. For example, posting content on social media, subscribing to a newsletter, leaving an online review or shopping online increases the size of our digital footprint.

Our contribution to digital footprint may not always be obvious. For example, websites can track the activities through the installation of cookies on our device, and apps can collect data without our knowledge. Organisations may sell or share personal information with third parties if they have access to it. Even worse, that personal information could get compromised if a breach occurs.

It is easy for social media services to track interactions between users, as long as they take place on their own services. For instance, it's obvious Instagram keeps track of which users' posts we respond to and uses the data collected in its news feed algorithm.

However, it is more difficult for them to track user activity on applications outside of social media. For example, links to social media posts and news are increasingly shared on so-called dark social media, which mainly refers to messaging apps such as WhatsApp.

Personal and relevant content is often generated when using online services and applications. Data about us is collected with every post, like and comment. We can also communicate with other users, especially on social media services. As a result, fraudsters and cybercriminals often target user accounts.

The EU's General Data Protection Regulation (GDPR) gives users many rights in relation to the use of services in the EU. Users have the following rights when personal data is processed on the basis of the user's consent or acceptance of the terms and conditions, i.e. a contract:

1.   The right to be informed about the processing of personal data.
2.   The right to access his/her personal data
3.   Right to rectify inaccurate data
4.   Right to deletion of personal data
5.   Right to be forgotten

Unfortunately, the data that emerged from the 2023 research, as well as those we collected in 2019, are not at all encouraging, and much still needs to be done by institutions to inform citizens of the risks they run when operating online, whether conducting financial transactions or simply socialising via the most varied applications on the market. There is a need to promote campaigns and projects that focus on online safety and the full assimilation of the Digital Footprint concept.

As European Digital Learning Network ETS, it is our hope to be at the forefront of this challenge together with our EU partners. In order to encourage and launch bottom-up initiatives, we want to step up our efforts to promote a broad dialogue with all stakeholders, civil society, EU institutions and European stakeholders. We need education and information activities to spread knowledge about these sensitive issues to all European citizens.

1. About the organiser/promoter

The European Digital Learning Network ETS – DLEARN – **aims to embrace the challenges brought by the digital transformation in terms of digital skills mismatch and digital learning opportunities.** The 47% of Europeans is not properly digitally skilled, yet in the near future 90% of jobs will require some level of digital skills.

We believe in the value of SHARING, CONNECTING, MULTIPLYING and ENHANCING the potential of our members, local territories and people.

Constant changes in economy and society have been urging governments to emphasize the contribution of education to a wide range of newly required skills and competencies. 21st Century skills are considered to be key enablers of responsible citizenship in an ICT-based economy.

A successful education and training in our knowledge society depends increasingly on the confident, competent and innovative use of ICT.

DLEARN wants to bring closer the experiences and voices of local territories and people to EU policies. Nowadays this process is hindered by the presence of bigger interests, notably big corporations or umbrella organizations. With our activities and through our network we want to minimize this gap, through the promotion of bottom-up initiatives, such as:

- Closer cooperation and enhancement of our activities to a higher level through periodic project labs;
- Tight networking activities and lobbying to achieve a fruitful accreditation of local needs to the relevant EU Commission DGs;
- Improving existing experiences and knowledge of digital learning through sharing of practices and creation of efficient business opportunities.

DLEARN is a **network made of members based all over Europe**, related to the field of Education & Training and ICT. In the framework of our activities, DLEARN – in cooperation with some of the most influent stakeholders in Europe in the sector of education and digital – promoted a survey to collect data to analyse EU citizens' understanding of digital footprint, that is the set of data that an individual creates through his or her online actions. Almost all online activities leave some form of digital trace.
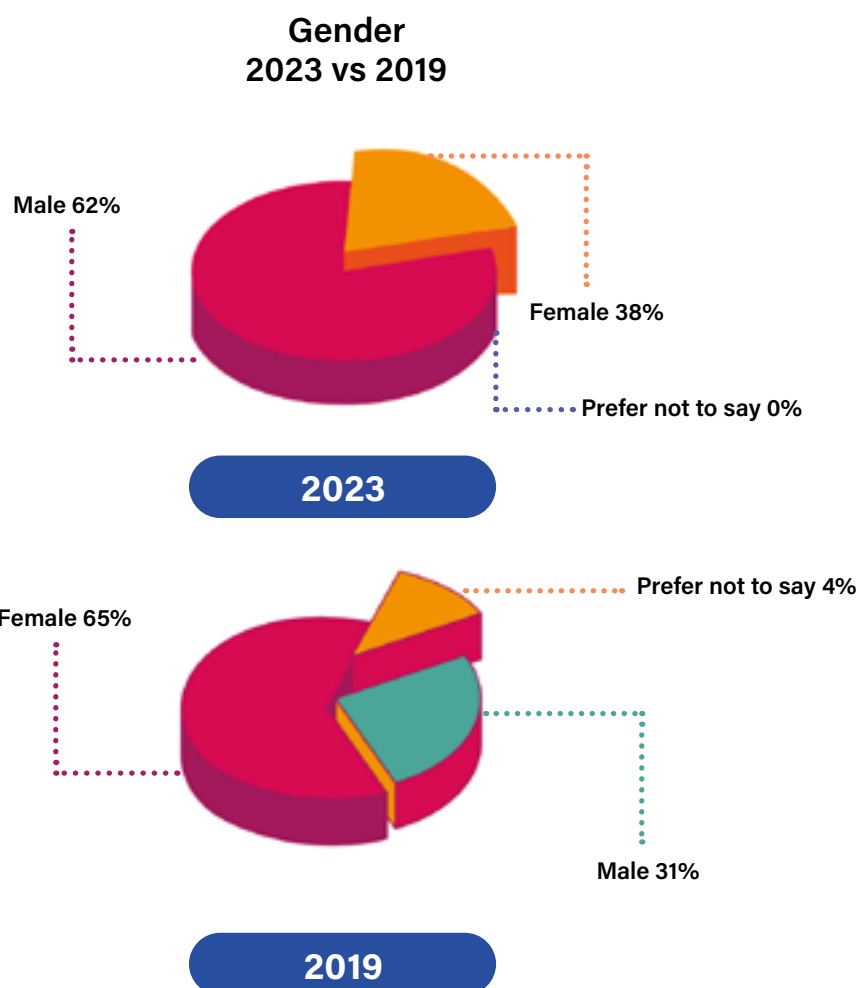
A digital footprint is relatively permanent and once the data is public - or even semi-public, as in the case of social media - the owner has little control over how it is used by others. This is the main reason why citizens must be aware of all the risks that can occur when they operate online.
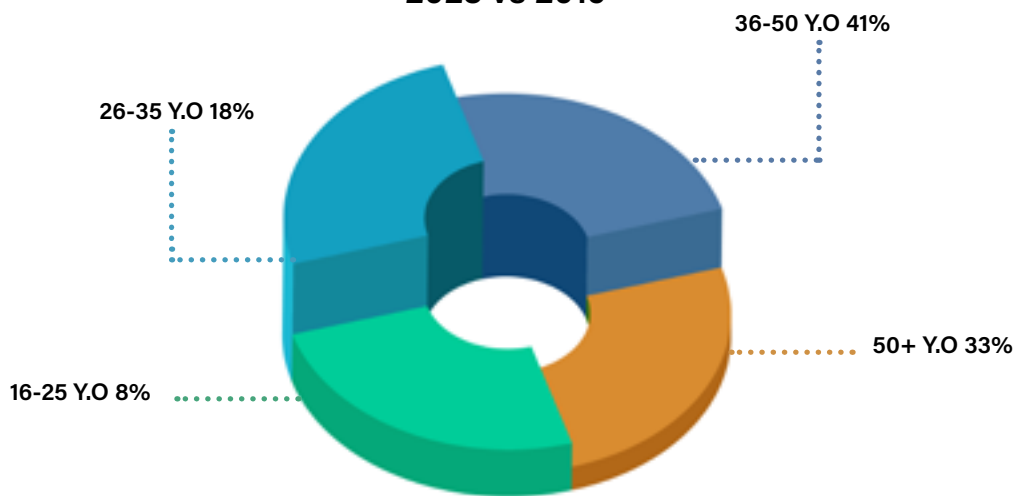
2. Respondents' demographic

The online survey was launched in May 2023 and kept live until September 2023 by the European Digital Learning Network ETS. The survey was distributed through all possible communication channels in 24 European languages to facilitate the collection process and to obtain as many responses as possible from European citizens: Albanian, Bulgarian, Finnish, French, German, Greek, Hungarian, Italian, Polish, Romanian, Slovenian and Spanish. It was widely disseminated by the European Digital Learning Network ETS, its members and partners of the initiative.

In 7 months, **we collected a total of 10.552 responses;** the first set of questions in the survey were dedicated to draw the profile of respondents. 4025 (the 38%) answers were given from women, while the 68%, i.e. 6517 of respondents were men. This is the first difference we found compared to the analysis conducted in 2019, where male respondents accounted for 31% and female respondents for 65%.

Gender
2023 vs 2019

Male 62%

Female 38%

Prefer not to say 0%

2023

Prefer not to say 4%
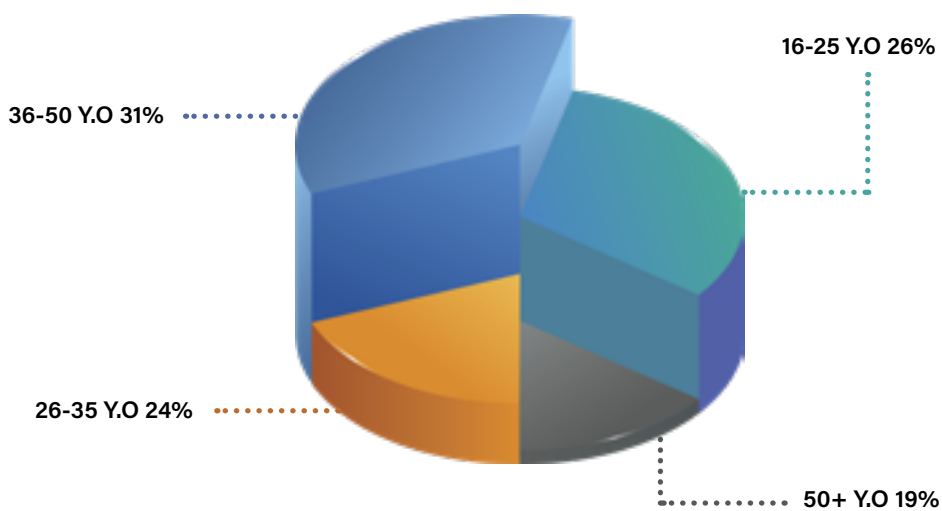
Female 65%

Male 31%

2019

As for the age range, the 41% of respondents (4343) are aged between 36 and 50 years old, 3520 answers came from people aged 50+ years old (the 33%), while 1900 respondents are between 16 to 35 years old (the 18%). Our sample therefore is mainly represented by adult people; in contrast to what we analysed in 2019, in this new research we have noticed a change with regard to the age and occupation of our respondents; contrary to the last edition, when we only publicised the research via social channels, this time we adopted a different method, relying not only on social publicity but also distributing paper questionnaires at various meetings, gatherings, seminars and other opportunities to meet, thus increasing the plethora of respondents and raising the average age and level of education of the people who answered our survey, as can be seen in the graphs below. Our respondents have a high level of education: Higher Education - 57% and Postgraduate – 25%;

AGE
2023 vs 2019

36-50 Y.O 41%

26-35 Y.O 18%

50+ Y.O 33%

16-25 Y.O 8%

2023

16-25 Y.O 26%

36-50 Y.O 31%

26-35 Y.O 24%

50+ Y.O 19%

2019

LEVEL OF EDUCATION
2023 vs 2019

Postgraduate
25%

Higher ed. (University)
57%

Secondary ed.
18%

2023

Postgraduate 24.7%

Secondary ed. 23.4%

First level of
compulsary
education 2.6%

Higher ed. (University)
57%

2019
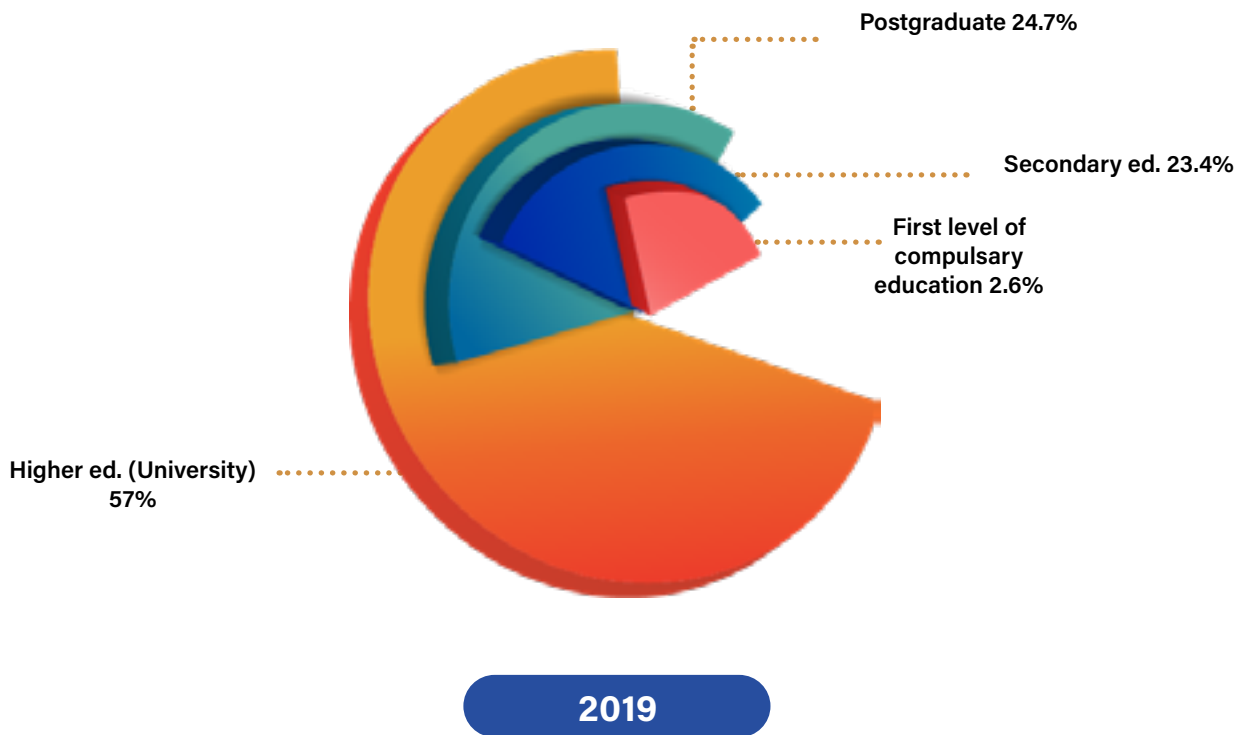
We also investigated their level of digital competence, which overall turned out to be more than good, where the 71% of the respondent have an intermediate level of competence while the 20% believes to have advanced competencies. The data we have collected in the 2023 edition are more or less the same we have analysed in the 2019, as we can see from the graphs below.

Technical Skill
2023 vs 2019

Basic
9%

Advanced
20%

71% Intermediate

2023

Basic 5%

Advanced 20%

75% Intermediate
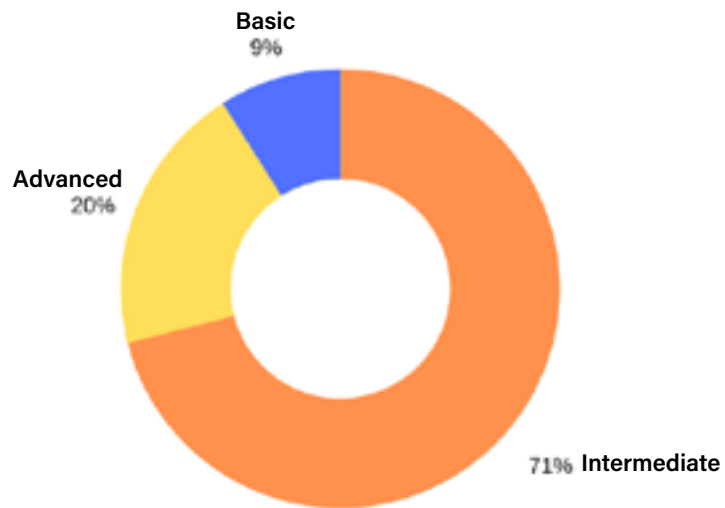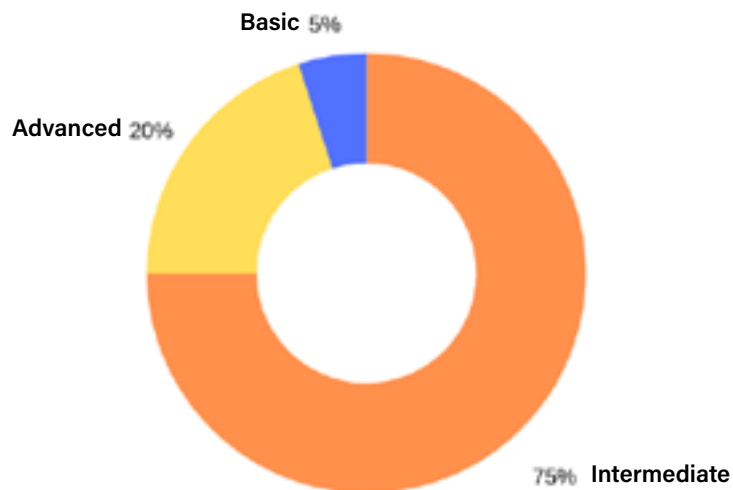
2019

The question about their country of origin clearly show how we succeeded in having a good representation from many European Member States, such as:

3. Level of understanding

The previous paragraph told us that our average interviewee was a **well-educated male between the ages of 36 and 50. He perceives himself as a digitally skilled user of various online services such as social media, online shopping platforms, etc. He works and lives in continental Europe.**

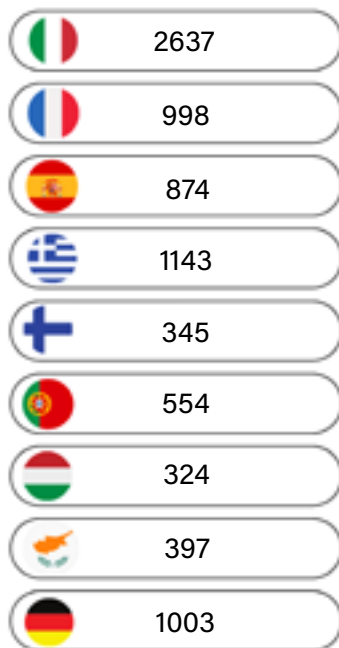When we ask whether respondents read the privacy policy in full before agreeing to it when registering for a new account or subscribing to a web portal, however, **the majority - 70% - say "yes,sometimes"** while 30% say "No". This is confirmed by the results of the next question. In fact, when asked whether they give third parties permission to use their personal data, 76% answered in the affirmative. The answer to this question has totally changed in its first part compared to 2019, where only 14% stopped to read the privacy policy in full before giving consent, while 80% of respondents said they did not pause but clicked directly on consent. Whereas now most respondents seem to read the privacy policy in full before giving consent anyway.

Privacy Policy Reading
2023 vs 2019

Yes, always
0%

No 30%

70% Yes, I do sometimes

2023

Yes, always
5%

Yes, I do sometimes 15%

80% No

2019
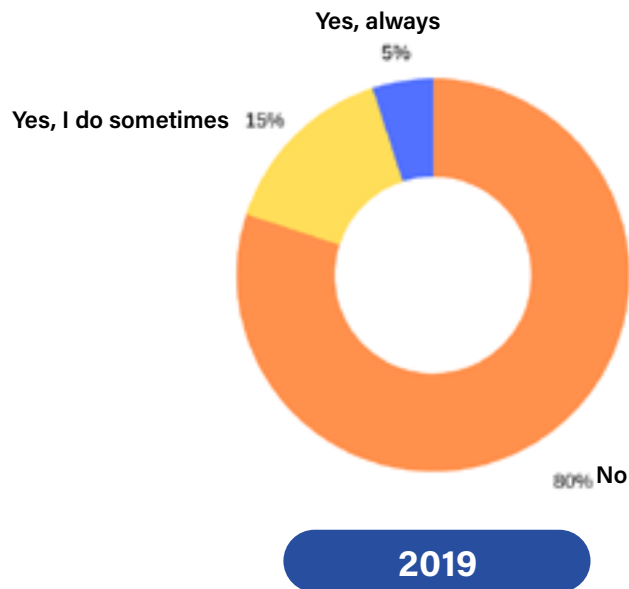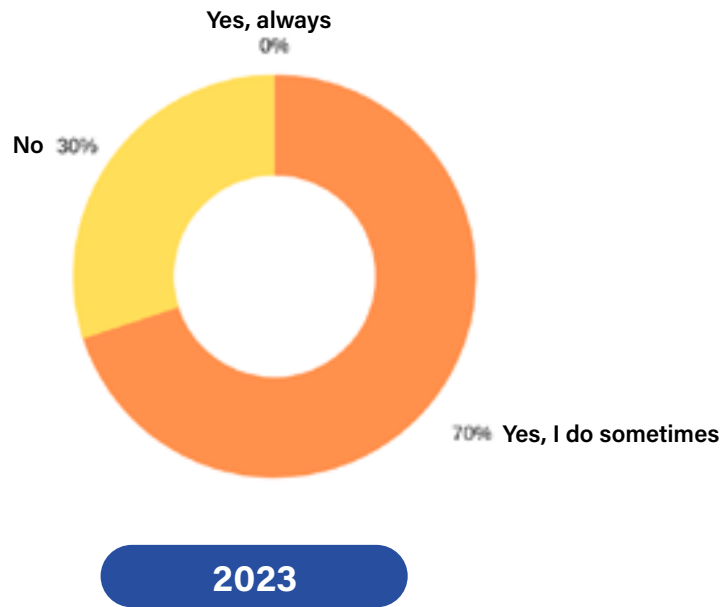
Moreover, **respondents seem to be not fully aware about who owns their trail of data** produced when navigating online. In fact, the 51% of the respondents affirmed that the data are owned just by companies to whom they have given unequivocal permission; while just the 29% said that these data are owned by private companies like Facebook, Instagram etc.

Who owns and can use the data about our behavior online

2023 vs 2019
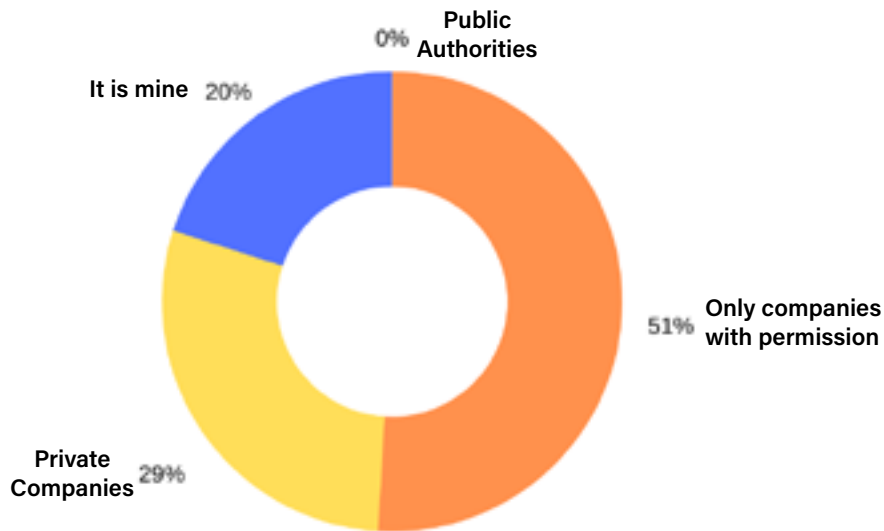
2023

However, the majority of people affirmed to have searched for their name on Google – 76%, of the respondents while only the 9% of them didn't care.

Have you ever searched your ''name/surname'' on Google to check your online identity and reputation?

2023
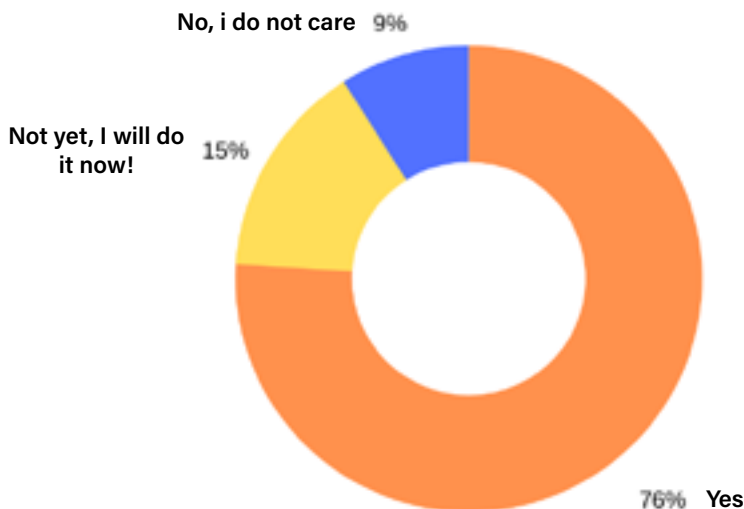
2023

4. Knowledge

In order to analyse citizens' current level of knowledge about digital footprint, digital identity and online reputation, the third set of questions in the survey was designed. First, we asked people to rate a statement as true or false.

From the chart below, we can learn that **most of the respondents think they don't have full control over their digital**, also worrying about other people who aren't aware of the implication of the digital footprint.
Additionally, **they are aware that other people can damage their online reputation by through false and harmful behaviour.**
Finally, respondents understood that online reputation is not only linked to social media but also to their activities through emails and navigation online.
Comparing with the same answers from the 2019 survey, we can see from the graph that no substantial changes were evident.

Results 2023

	TRUE	%	FALSE	%
I am in full control and i am able to manage my digital identity	3898	37%	6654	63%
Me, i am fine, but i know many people who are completely unaware	8719	83%	1833	17%
Someone could easily influence my online reputation by posting fake information under my name	7502	71%	3050	29%
If you just send emails and visit websites you don't have to worry about your online reputation	776	7%	9776	93%

Results 2019

	TRUE	%	FALSE	%
I am in full control and i am able to manage my digital identity	5832	29%	13896	70%
Me, i am fine, but i know many people who are completely unaware	13535	68%	6193	31%
Someone could easily influence my online reputation by posting fake information under my name	14529	73%	5199	26%
If you just send emails and visit websites you don't have to worry about your online reputation	1794	9%	17934	90%

Respondents began to think about the use of their data, as can be seen from these responses. They also began to **understand that they could exercise power over their personal data** as they navigated the web. In fact, when asked about how they think their profile should be used, a large number of respondents, the 39%, were for "My data are just mine, it should not be used for any purpose" while none believes that Private companies, including social media platforms, can sell their data as they wish.

Use of the personal profile

2023

To be made available to national security agencies 12.9%

Private companies can sell my data 0%

My data are just mine 34.4%

In the public interest 25.8%

To suggest items that I possibly want to buy 8.6%

To check their future employees' online profiles 18.3%
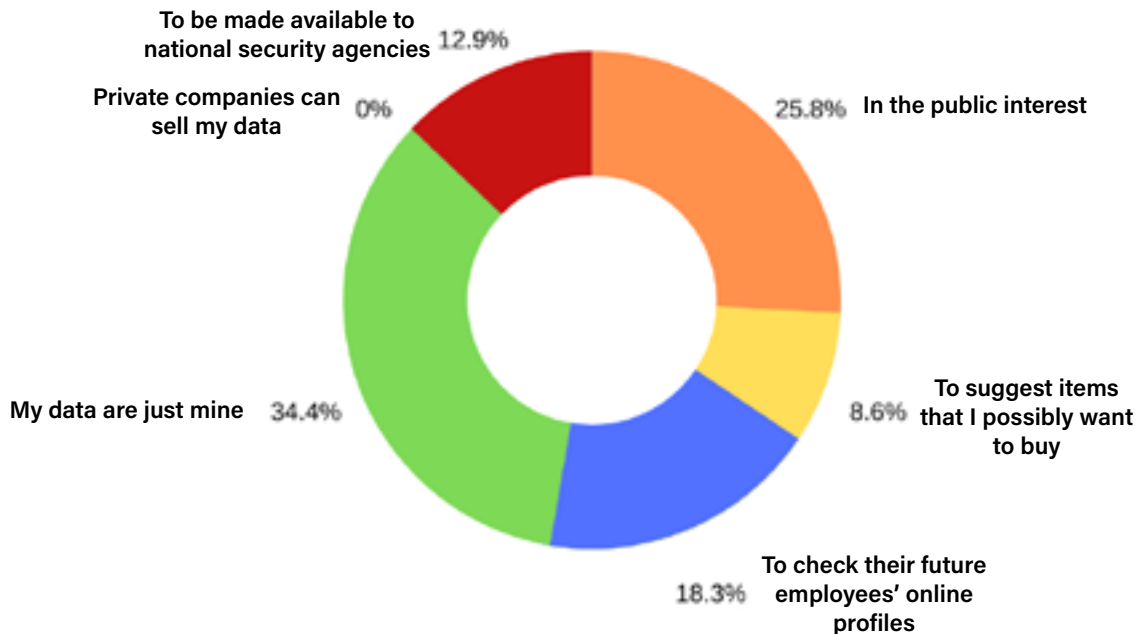
2023

When it comes to what a prospective employer might look for online regarding a new employee, respondents believe that **anything posted on the web can be evaluated,** as we can see from the graph below, without one particular action taking precedence over the others.

Activities that could impact on the employer's decision to hire you

2023

It is unfair for an employer to look at my online reputation 14%

Your political beliefs expressed online 13%

Poor grammer in comments and posts 13%

Negative comments about previous employers 21%

The photos and videos you have published 21%

The pages you follow on your social media 18%
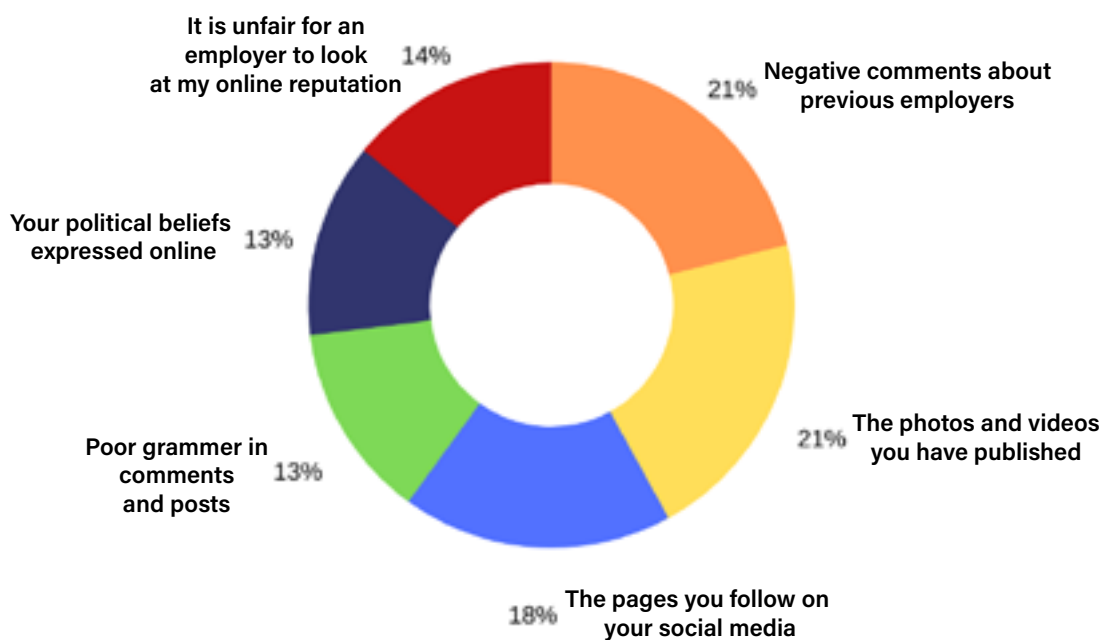
2023

In terms of **promoting their own reputation online**, respondents agreed that they should be more careful when posting online - 67% and only the 15% of the respondent believes that once you post something online it can't be removed. However, they **are fully aware that personal data online can be breached** – 86% while the 14% believes that this possibility is rare.

Revise online reputation
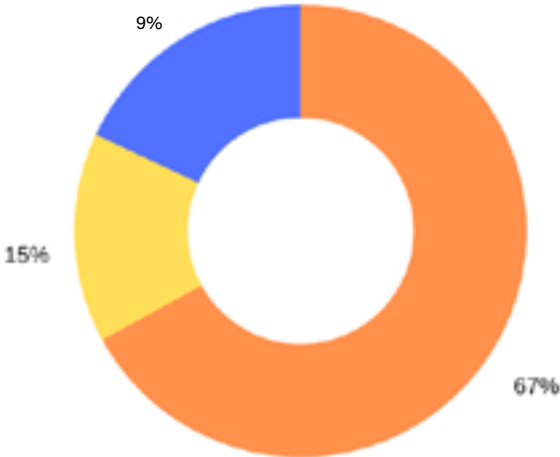
2023

2023

Online personal data might be subject of breach

2023

2023

5. Taking action

Finally, citizens were asked what they do to protect their personal data and what they will do to use the Internet safely.

The majority of respondents - 53% - said they would be particularly careful about disclosing financial information, while 20% said they would protect their identity, name, nationality and address.

Online personal data to be protected

2023

Shopping preferences 9%

Web browsing history 18%

My identity name,
nationality, address, etc.. 20%

53% Financial information
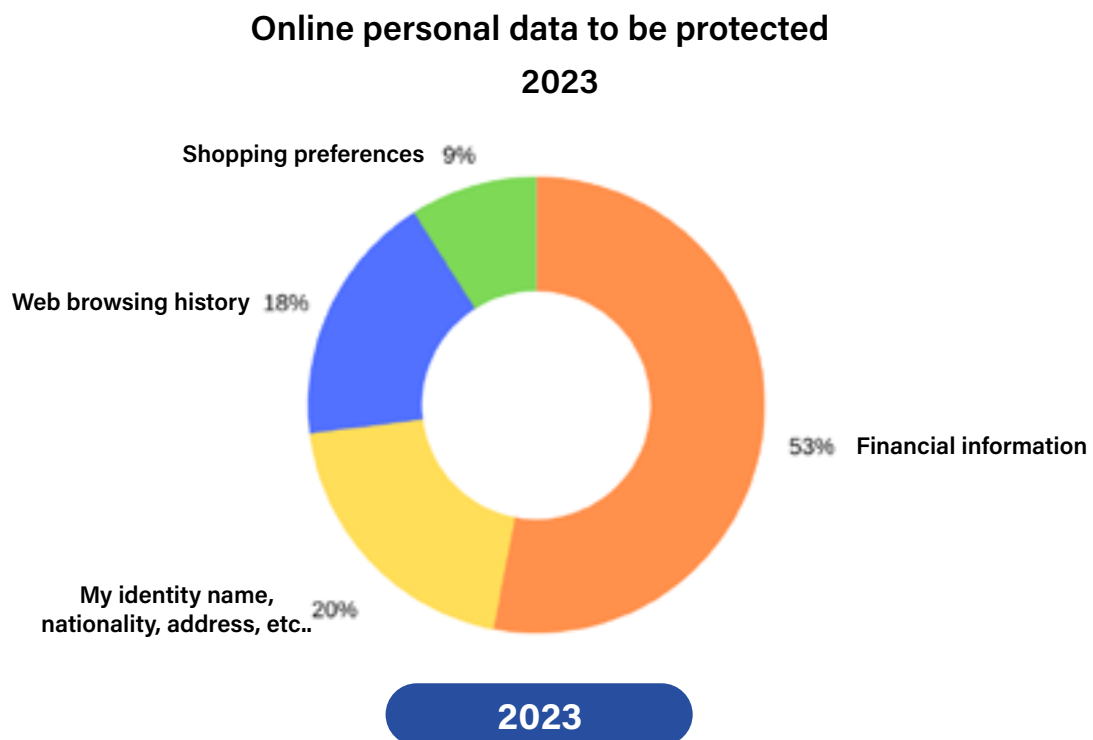
2023

Few people protect their surfing history and shopping habits. Findings on whether people have recently changed their device settings confirm this.

Adjustments on devices
Results 2023

	YES	%	NO	%
Location tracking	8556	81%	1986	19%
Privacy settings on social media	8536	81%	2016	19%
Change username/password or delete your old media accounts	6600	63%	3952	37%
Private mode in your browser	5800	55%	4752	45%
Anti-tracking tools	3048	29%	7504	71%
Ads block software	5262	50%	5290	50%
None of the above	196	2%	10356	98%

Adjustments on devices
Results 2019

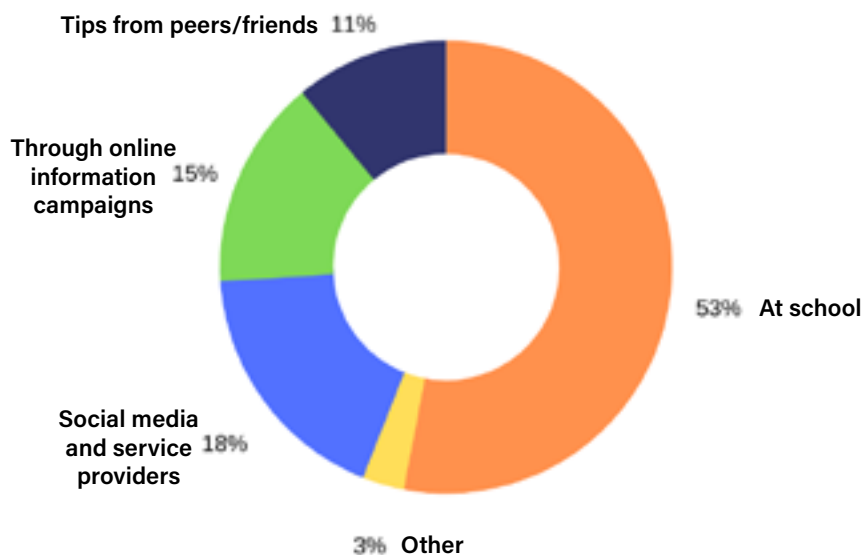|	YES	%	NO	%
Location tracking	14328	72%	5399	28%
Privacy settings on social media	15407	78%	4320	22%
Change username/password or delete your old media accounts	13853	70%	5874	30%
Private mode in your browser	12809	64%	6918	36%
Anti-tracking tools	6981	35%	12748	65%
Ads block software	11613	58%	8114	42%
None of the above	2175	11%	17552	89%

While most people have adjusted their location tracking and privacy settings, few have used ad blocking or tracking tools.

Respondents are willing to learn more and want to acquire the right skills in order to how best to take action for mindful internet use. Most of them would like to learn more of these skills at school - 53%, the 18% believes that social media companies should be obliged to provide this opportunity; while the 15% prefers to be informed via online information campaigns.

This data is different if compared with the data analysed in 2019, in accordance also with the background of the respondents. It seems in fact that people around 50 years old believes that the schools should be responsible for the education of people also regarding how to operate online, while the respondents between 16 and 35 years old believe that the social media and service providers should be obliged to provide more user-friendly support, as shown by the graphs below.

Where to learn the right skills to manage the online reputation
2023

Tips from peers/friends 11%

Through online information campaigns 15%

53% At school

Social media and service providers 18%

3% Other

2023

Where to learn the right skills to manage the online reputation
2019

Other — 5.8%
Social media and service providers — 15.6%
At school — 27.2%
Through online information campaigns — 23.3%
Tips from peers/friends — 28%
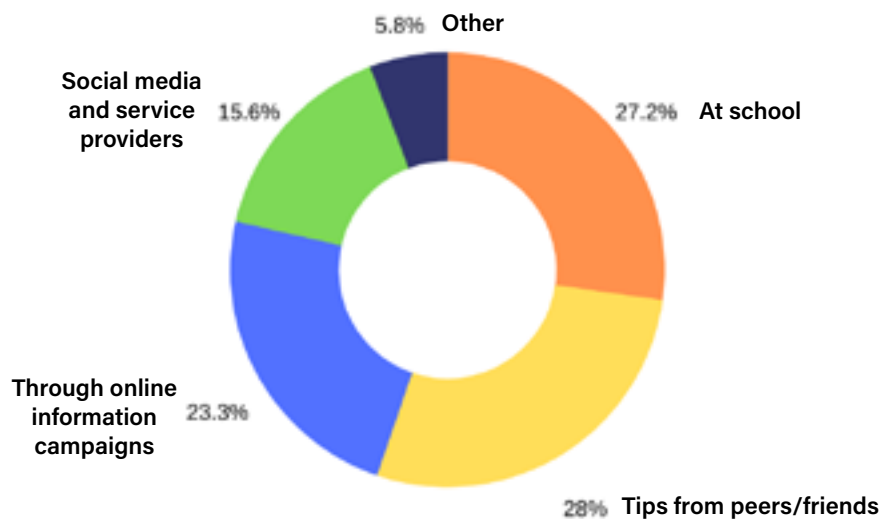
2019

Finally, the table below shows what respondents think about social media behaviours and possible actions they can take to improve security and positive behaviour.
Most of respondents think that **social media also should comply with stricter regulations (63%)** while users should be given more control over their data, including option to delete it (20%).

Possible actions to improve security and positive behaviour online
2023

Social Media Platform

Social media platforms and service providers should comply with stricter regulations

63%

Code of Conduct

It would be sufficient if they would adhere to a code of conduct and regulate themselves

10%

User's Responsability

Users are the sole responsible of their behaviour online, no regulations at all

7%

More control to users

Users should be given more control over their data, including the option to delete it

20%

6. Conclusion

Thanks to the data we obtained from this 2023 survey, and by comparing it with the data obtained during the first edition of the 2019 report, **we can accurately profile the average citizen who uses the internet and his awareness of his digital footprint and how it affects his reputation on the web.**

6.1 The Respondent's Demographic

6.1.1 The Data

THE RESPONDENT'S DEMOGRAPHIC

1 **Gender**

The 68% of the respondents are MEN.

The 38% of the respondents are WOMEN.

2 **Age**

41% : 36 - 50 Years Old

33% : 50+ Years Old

18% : 16 - 35 Years Old

3 **Education Level**

According to the answers, our respondents have a high level of education

57% : Higher Education
25% : Post Graduated

4 **Digital Competence**

71% Have an intermediate level of digital competence
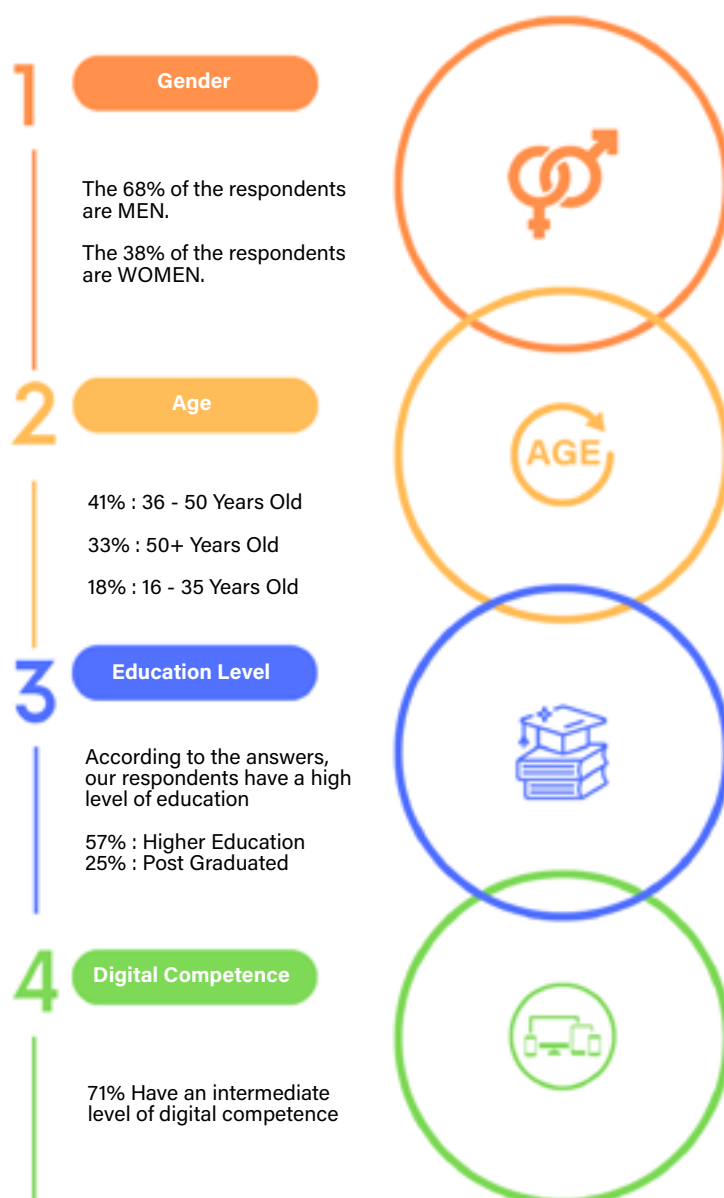
6.1.2 The Analisys

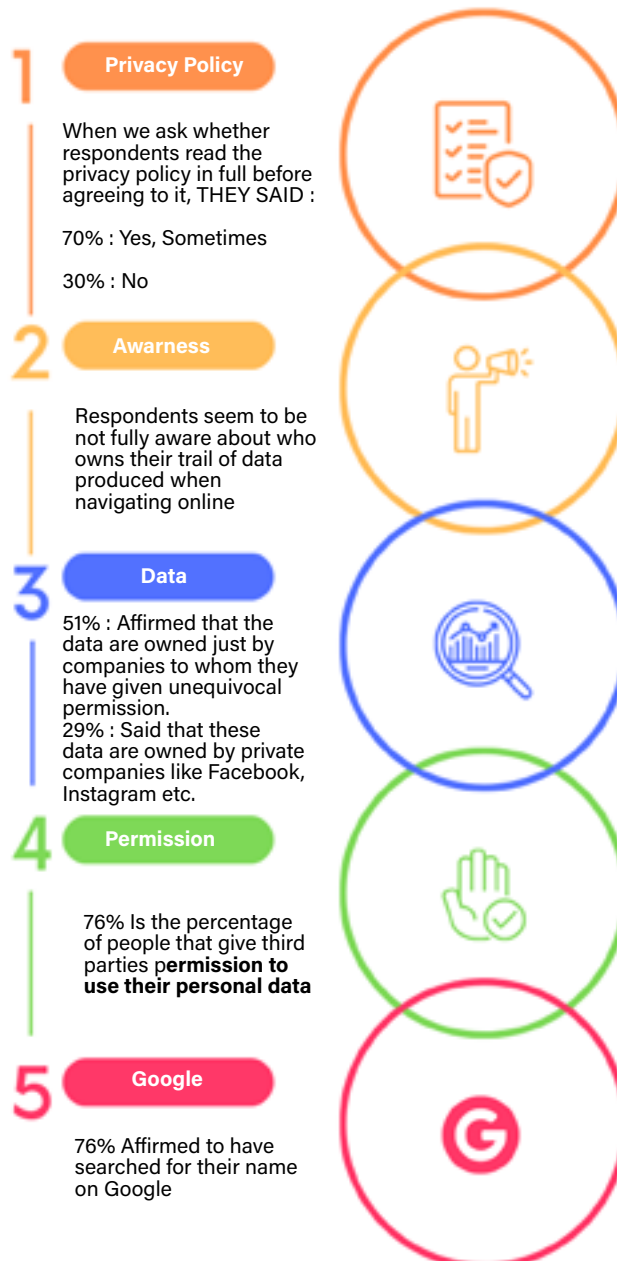The portrait of the average user that we obtained from the analysis of the data collected during the research phases, shows a male user, over 36 years old, with a high level of education ranging from a bachelor's degree to a postgraduate master's degree. The digital skills he believes he has, are intermediate to high. This denotes that people with the above-mentioned characteristics are more interested in the notion of DIGITAL FOOTPRINT and are also interested in all the practices related to it, as they recognise that risks can be easily avoided through greater knowledge of digital tools.

6.2 The level of understanding

6.2.1 The Data

THE LEVEL OF UNDERSTANDING

1 Privacy Policy

When we ask whether respondents read the privacy policy in full before agreeing to it, THEY SAID :

70% : Yes, Sometimes

30% : No

2 Awarness

Respondents seem to be not fully aware about who owns their trail of data produced when navigating online

3 Data

51% : Affirmed that the data are owned just by companies to whom they have given unequivocal permission.
29% : Said that these data are owned by private companies like Facebook, Instagram etc.

4 Permission

76% Is the percentage of people that give third parties permission to use their personal data

5 Google

76% Affirmed to have searched for their name on Google

6.2.2 The Analysis

As we can see from the data obtained during this research, the users, normally, read the privacy policy in full before giving their consensus but, in most of the cases, they give it anyway, even if they didn't read it in total, or carefully. This generates a lot of misunderstanding regarding the data protection in our respondents.

If it is obvious and normal to think that stolen data comes from a cyber-attack that allows attackers to get their hands on data hosted on servers and PCs, less well known is the means of online scraping. In the case of scraping, in fact, there is no abusive access to databases. On the contrary, data are plundered from social networks, private platforms, and various websites.

In this case, that is, tools are used to collect data already published on other platforms. An archive is then compiled, which then ends up for sale. In order to combat this type of phenomenon, which is becoming less and less rare, there needs to be particular care on the part of citizens when surfing the web and also greater care on the part of digital platforms in informing users of the possible risks.

> **We can say that most of user of 2023 are aware users who pay considerable attention to what their online presence entails, unfortunately, however, there are still situations that place them in a risky situation and expose them to possible online scams and dangers.**

6.3 The level of Knowledge

6.3.1 The Data

Most of the respondents think they don't have full control over their digital data (63%).

They are aware that other people can damage their online reputation through false and harmlful behaviour (71%).

People start understanding that they could exercise power over their personal data as they navigated the web

39% Affirmed that the data are private and they should not be used for any purpose

0% Believes that private companies, including social media platforms, can sell their data as they wish

When it comes to what a prospective employer might look for online regarding a new employee, respondents believe that anything posted on the web can be evaluated

67% Affirmed that everyone has to be more careful about when posting online

86% Are fully aware that personal data online can be breached

6.3.2 The Analysis

In this regard, citizens, from what emerged from our survey, believes that they don't have full control about their personal data and also are aware of the fact that what they post on social media and how they use it is much more important than one might imagine. The set of information we share online it is not private: it is public for millions of people and, above all, it is within the reach of recruiters, HR managers and even current and future employers.

> **What emerged from this research is that citizens are aware that all information shared online can be analysed by future employers and this determines their reputation not only online but also in real life. Therefore, respondents would like to have more training in how to behave online and would like this to start as soon as possible.**

Due to this condition, the respondents of this research **would appreciate education starting from school and then continuing through the major digital sharing and social platforms,** which must also take responsibility for warning and training their users so as to safeguard them from possible misbehaviour that may cause unpleasantness.

6.4 Taking Action

6.4.1 The Data

Citizens were asked that they do to protect their personal data and what they will do to use the Internet safely. The majority of respondents - 53% - said they would be particularly careful about disclosing financial information, while the 20% said they would protect their identity, name, nationality and address

Few people protect their surfing history and shopping habits - just the 18% and 9% of the respondents.

While most people have adjusted their location tracking and privacy settings, few have used ad blocking or tracking tools - 29% and 50%

Most of respondents think that social media also should comply with stricter regulations (63%) while users should be given more control over their data, including option to delete it (20%).

Respondets are willing to learn more and want to acquire the right skills in order to understand how best to take action for mindful internet use
53% : Affirmed that would like to learn more of digital skills at school
18% : Believes that social media companies should be obliged to provide this opportunity
15% : Prefers to be informed via online information campaigns

6.4.2 The Analysis

Through the data we collected in this last section of the research, we learned that the average citizen, aware of the potential risks of the web, tends to implement some basic strategies that make him or her feel safer when surfing online. Most of these actions relate to safeguarding data related to the financial sphere (avoiding sharing home-banking passwords, protecting credit card transactions or using insured payment platforms). The information about the history of the sites we visit is also hardly ever protected, but even this exposes us to the theft of important personal data about our habits and tastes.

Moreover, **it is essential to make citizens aware of the presence of 'active' or 'passive' activities that make up our Digital Footprint**; in fact, if active ones are easily recognisable and the object of attention by users, passive activities are less visible and more subject to risks. For instance, our surfing and browsing habits are part of our passive digital footprint, created without our knowledge and, sometimes, our consent, while actions on a social media are more likely to be considered an active digital footprint.

With the accessibility and availability of digital footprint data comes the need to become aware of how exposed one's footprint is and how vulnerable it is to cyber risks.

In conclusion, the issues related to the digital footprint are numerous. They permeate the lives of citizens in many ways. There are still gaps to fill, especially when it comes to explaining and communicating the importance of using online codes of conduct to protect our personal reputations and activities. Ultimately, the solution comes from the citizen directly : They need more assistance on how to manage their own digital footprint directly through social media, and more information through campaigns and education. People are calling for better information, more control over htier data and more control over companies that should be subject to more stringent rules

6.5 Comparison between 2019 and 2023's data

As mentioned above, the 2023 report is the second edition of the digital footprint report conducted by the European Digital Learning Network, the first edition being in 2019.

What we have noticed, compared to the previous edition, is that men have outnumbered women in terms of the number of responses obtained and the age of respondents has risen, while digital skills and level of education has remained more or less unchanged.

This indicates an increased interest in the digital footprint even among those who did now show much interest until a few years ago. The issue of one's digital footprint and the protection of personal data is becoming more and more topical, as is the need for all people who surf online to implement strategies to protect the sensitive information we make available on the web every day.

With regard to the level of understanding, compared to the 2019 edition, we did not find much difference except in the fact that, as of today, the majority of respondents read the privacy policy of the websites they browse at least sometimes, whereas in the 2019 edition, almost none of the respondents thought it was necessary to read the privacy policy. Despite this difference, however, the majority of citizens still give their consent to data processing. The same applies to the exclusive ownership of data, still too many people believe that data is their exclusive property, leading to great confusion among users.

> **We can therefore say that, as far as this section is concerned, there have been no major difference and that much still needs to be done in terms of educating citizens about sharing their data online and the safeguards that are available.**

With regard to citizens' knowledge when it comes to digital footprints, again there were no major changes from the previous edition in 2019.
We learned that the majority of respondents feel that they do not have full control over their digital footprint, and are also concerned about other people who are unaware of the implications of their digital footprint.
Furthermore, they are aware that other people can damage their online reputation through false and malicious behaviour.
Finally, respondents realised that online reputation is not only related to social media, but also to their activities through e-mail and online browsing.
This thus denotes a substantial awareness on the part of citizens of the risks that can occur when surfing the web, and that every action taken online also has repercussions in real life. It is therefore necessary to take action to improve and bring to the highest level the knowledge available to citizens, creating ad hoc campaigns that can help improve skills.

Finally, regarding the last section of the research, wanting to make a comparison between 2023 and 2019, we can see that the respondents are willing to learn more and want to acquire the right skills in order to understand how best to take action for mindful internet use. Most of them would like to learn more of these skills at school.

This data is different if compared with the data analysed in 2019, in accordance also with the background of the respondents. It seems in fact that people around 50 years old believes that the schools should be responsible for the education of people also regarding how to operate online, while the respondents between 16 and 35 years old believe that the social media and service providers should be obliged to provide more user-friendly support.

Taking this into consideration, we can say that citizens need to be educated as soon as possible, starting from schools and reaching the large online platforms. Moreover, although they are aware of the safeguards that the EU has put in place to protect their rights, they would like stricter rules to be put in place to protect their privacy and they would also like the power to be able to operate autonomously with regard to the use of their personal data, including the power to be able to remove it completely.

> **These data are fundamental because they show us a picture that is more or less unchanged compared to four years ago, and therefore there is a strong need to put in place new regulations in line with the needs of citizens, also by implementing a strong synergy between legislators and the major web giants.**

7. The Policy Recommendations

The European Digital Learning Network, having in mind the results of the survey described above and the feedbacks from the conference wants to call for:

> **Increasing educational opportunity for all**

While the individual is the primary data owner, he or she must understand the full impact. In the past few years, we have seen the emergence of many new initiatives, including the ET2020 digital literacy action plan: Learning, Teaching and Assessment (DELTA) and the Digital Competence Framework for Citizens 2.2 (2022 updated version). The update takes account of emerging technologies such as Artificial Intelligence, the Internet of Things and datafication or new phenomena such as the new teleworking conditions that have led to new and increased digital competence requirements on the part of the citizen. Therefore, **we propose to create a positive culture around their digital identity and the amount of personal data they share online by improving personal data education opportunities from primary school onwards and raising awareness among children, parents and teachers.**

> **Simplification of cyber security implementation solutions**

Simplify the implementation of cybersecurity solutions Citizens must protect themselves and their families when navigating online, but tools should be easy to use and apply, especially for children. On the 18 April 2023, the European Commission proposed the EU Cyber Solidarity Act, to improve the response to cyber threats across the EU. The proposal will include a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism to create a better cyber defence method. To that end, it is suggested that the certification framework for digital goods should also become accountable and comprehensible to all European citizens, so that it becomes a point of reference for the choice of digital goods, like other European labels such as the EU Eco-label or the organic label. The Commission prepared a call for coherent framework for teaching cybersecurity skills in university and professional education. The four pilot projects that prepare the cybersecurity competence centre and network by ECSO are currently working on this. There are also recurring initiatives meant directly for students, such as the yearly European cybersecurity challenge.

Cybersecurity skills fall under the Commission's general agenda on digital skills. They are also a part of the funding efforts under Horizon 2020, Horizon Europe and the Digital Europe Programme. One example is the funding for 'cyber ranges', which are live simulation environments of cyber threats for training. This is why **we are proposing to encourage EU citizens to think critically when they read or post something online by means of simple learning pills that they can have at their disposal online at any time and in any place.**

Promoting a positive online culture

As people navigate online, they continue to act as citizens offline. **Our proposal is to encourage EU citizens to think critically when reading or posting something online by means of simple learning tools that are available online, anytime and anywhere.**

Bringing social media closer to citizens

In 2018, 56% of people aged 16 to 74 participated in social networks in the EU (Eurostat 29/06/2019). Since the beginning of data collection (38% in 2011), the participation rate in social networks in the EU has increased steadily. Therefore, the EU puts much effort into media literacy policies, such as tackling online disinformation, the Media Literacy Expert Group and the Audiovisual Media Services Directive. In the dialogue between people and social media companies, institutions must be accountable to their citizens. **We therefore propose the creation of a platform where European institutions, citizens and businesses can work together to encourage citizens to become more aware of online abuse and misinformation.**

8. Annexes

8.1 The Questionnaire "Digital Footprint Awareness"

Digital Footprint Awareness

A digital footprint is the trail of data you leave behind when you do something online. Awareness is the precursor to becoming media literate and to be able to participate fully in modern society. It is also a necessary pre-condition of acquiring technical skills (often referred to as digital literacy) and cognitive skills (the capacity to make sense of information and understand the implications of online activity).
Are people aware, for instance, of how their identity and reputation is tracked online? This survey is designed to collect data relating to individuals' awareness about their digital footprint. It will also assess the current and desired level of control exercised by citizens over their digital footprint, as well as the protections and safeguards they would like to implement in the future. The final report will be shared and discussed with the European Commission and freely available for everyone.

This research is run by DLEARN - European Digital Learning Network ETS.

Section: GENERAL INFORMATION

01. GENDER: ◯ Male ◯ Female ◯ Prefer not to say

02. HOW OLD ARE YOU? ◯ 16-25 ◯ 26-35 ◯ 36-50 ◯ 50+

03. WHAT IS THE HIGHEST LEVEL OF EDUCATION YOU HAVE COMPLETED?

◯ First level of compulsory education ◯ Secondary education ◯ Higher education (University) ◯ Postgraduate

04. MY TECHNICAL SKILLS ARE:

◯ BASIC (USING AN INTERNET BROWSER, SENDING AND RECEIVING EMAILS, WORD PROCESSING)

◯ INTERMEDIATE (SHOPPING ONLINE, USING SOCIAL MEDIA, USING GRAPHICS AND MULTIMEDIA)

◯ ADVANCED (ADVANCED USE OF DATABASES, PROGRAMMING AND SCRIPTING)

05. WHAT IS YOUR COUNTRY OF RESIDENCE? ....

06. WHAT IS YOUR OCCUPATION: ◯ I am a student ◯ Professionally occupied
◯ I do not work ◯ I am retired

Section: DIGITAL FOOTPRINT AWARENESS

07. **HAVE YOU EVER READ A PRIVACY POLICY IN FULL BEFORE AGREEING TO IT?**

    ◯ Yes, I do sometimes   ◯ Yes, always   ◯ No

08. **HAVE YOU EVER GIVEN PERMISSION FOR THIRD PARTIES TO ACCESS AND USE YOUR DATA?**

    ◯ Yes   ◯ No

09. **WHO OWNS AND CAN USE THE DATA ABOUT YOUR BEHAVIOR ONLINE, SUCH AS YOUR CONTACTS OR YOUR LOCATIONS?**

    ◯ It is mine, no one should use it

    ◯ Private companies such as Facebook/Instagram/Google, for instance, to store and use my data to create my online profile

    ◯ Only companies to whom I have given my unequivocal permission

    ◯ Public authorities which promote public interest

    ◯ Anyone who wishes, those data are not mine anymore

Section: ONLINE REPUTATION

10. **HAVE YOU EVER SEARCHED YOUR "NAME/SURNAME" ON GOOGLE TO CHECK YOUR ONLINE IDENTITY AND REPUTATION?**

    ◯ Yes   ◯ Not yet, I will do it now   ◯ No, I don't care

11. **PLEASE, INDICATE IF THE FOLLOWING SENTENCES ARE "TRUE OR FALSE" ACCORDING TO YOUR BEST KNOWLEDGE:**

    TRUE　**FALSE**

    ◯　◯　I am in full control, and I am able to manage my digital identity

    ◯　◯　Me, I am fine, but I know many people who are completely unaware

    ◯　◯　Someone could easily influence my online reputation by posting fake information under my name

    ◯　◯　In any case if people don't use social media, but only email or the internet they don't have to worry about their online reputation

12. **HOW DO YOU THINK YOUR PROFILE SHOULD BE USED?** *TICK AS MANY AS APPLY*

    ◯ When employers check their future employees' online profiles

    ◯ To suggest items that I possibly want to buy

    ◯ In the public interest (for instance for research or educational purposes)

    ◯ To be made available to national security agencies

    ◯ Private companies, including social media platforms, can sell my data as they wish

    ◯ My data are just mine, it should not be used for any purpose!

13. WHICH OF THE FOLLOWING ONLINE ACTIVITIES DO YOU THINK COULD IMPACT AN EMPLOYER'S DECISION TO HIRE YOU? *TICK AS MANY AS APPLY*

- Negative comments about previous employers
- The photos and videos you have published
- The pages you follow on your social media
- Poor grammar in comments and posts
- Your political beliefs expressed online
- It is unfair for an employer to look at my online reputation

14. HOW CAN I REVISE AND PROMOTE MY ONLINE REPUTATION TO MY ADVANTAGE?

- I can always delete something I have published
- I can promote a positive reputation
- I can be more mindful of what I publish online
- You cannot, once something is published online it cannot be removed

15. DO YOU THINK THAT YOUR ONLINE PERSONAL DATA MIGHT BE SUBJECT OF BREACH?

- Yes
- It is rare
- It is impossible to steal data online

16. ARE YOU AWARE THAT YOUR ONLINE ACTIVITIES (SURFING THE INTERNET, USING SOCIAL MEDIA, SHOPPING ONLINE) ARE TRACKED IN ORDER TO BUILD YOUR ONLINE PROFILE AND REPUTATION?

- Yes
- No

Section: MEDIA LITERACY COMPETENCES

17. WHICH OF THE FOLLOWING PERSONAL DATA DO YOU KEEP PROTECTED? *TICK AS MANY AS APPLY*

- My identity name, nationality, address, etc.
- Web browsing history / behaviour preferences
- Shopping preferences
- Financial information, e.g. credit cards or bank accounts numbers

18. HAVE YOU RECENTLY USED ANY OF THE FOLLOWING TOOLS OR MADE ANY OF THE FOLLOWING ADJUSTMENTS ON YOUR DEVICES?

YES	NO	
		Location tracking
		Privacy settings on social media
		Change username/password or delete your old media accounts
		Private mode in your browser
		Anti-tracking tools
		Ads blockers software
		None of the above

19. WHERE SHOULD I LEARN THE RIGHT SKILLS TO MANAGE MY ONLINE REPUTATION? *TICK AS MANY AS APPLY*

- ⬤ At school
- ⬤ Tips from peers/ friends
- ⬤ Through online information campaigns
- ⬤ Social media and service providers should be obliged to provide more user-friendly support
- ⬤ Other

Section: WHAT YOU CAN DO TO BETTER PROTECT YOURSELF?

20. FOR WHICH OF THE FOLLOWING PURPOSES SHOULD YOUR DATA BE USED? *TICK AS MANY AS APPLY*

- ⬤ For employers to check their future employees' online profiles
- ⬤ To suggest items that I possibly want to buy
- ⬤ To be made available to national security agencies
- ⬤ Private companies such as Facebook can sell as they wish my data
- ⬤ My data are just mine, it should not be used for any purpose!
- ⬤ In the public interest (for instance for research or educational purposes)

21. WOULD YOU BE IN FAVOUR OF THE FOLLOWING?

- ⬤ Social media platforms and service providers should respect stricter regulations
- ⬤ It would be sufficient if they follow a code of conduct and regulate themselves
- ⬤ Users are the sole responsible of their behavior online, no regulations at all
- ⬤ Users should be given more control over their data, including the option to delete it

22. DO YOU HAVE ANY FURTHER COMMENTS OR IDEAS YOU'D LIKE TO SHARE?

....
....
....
....

IF YOU WOULD LIKE TO STAY INFORMED ABOUT THE RESEARCH AND ITS RESULT, PLEASE LEAVE HERE YOUR CONTACT:

NAME/FAMILY NAME ....

ORGANIZATION ....

COUNTRY ....

EMAIL ADDRESS ....

www.dlearn.eu

Thank you very much for answering the questionnaire!