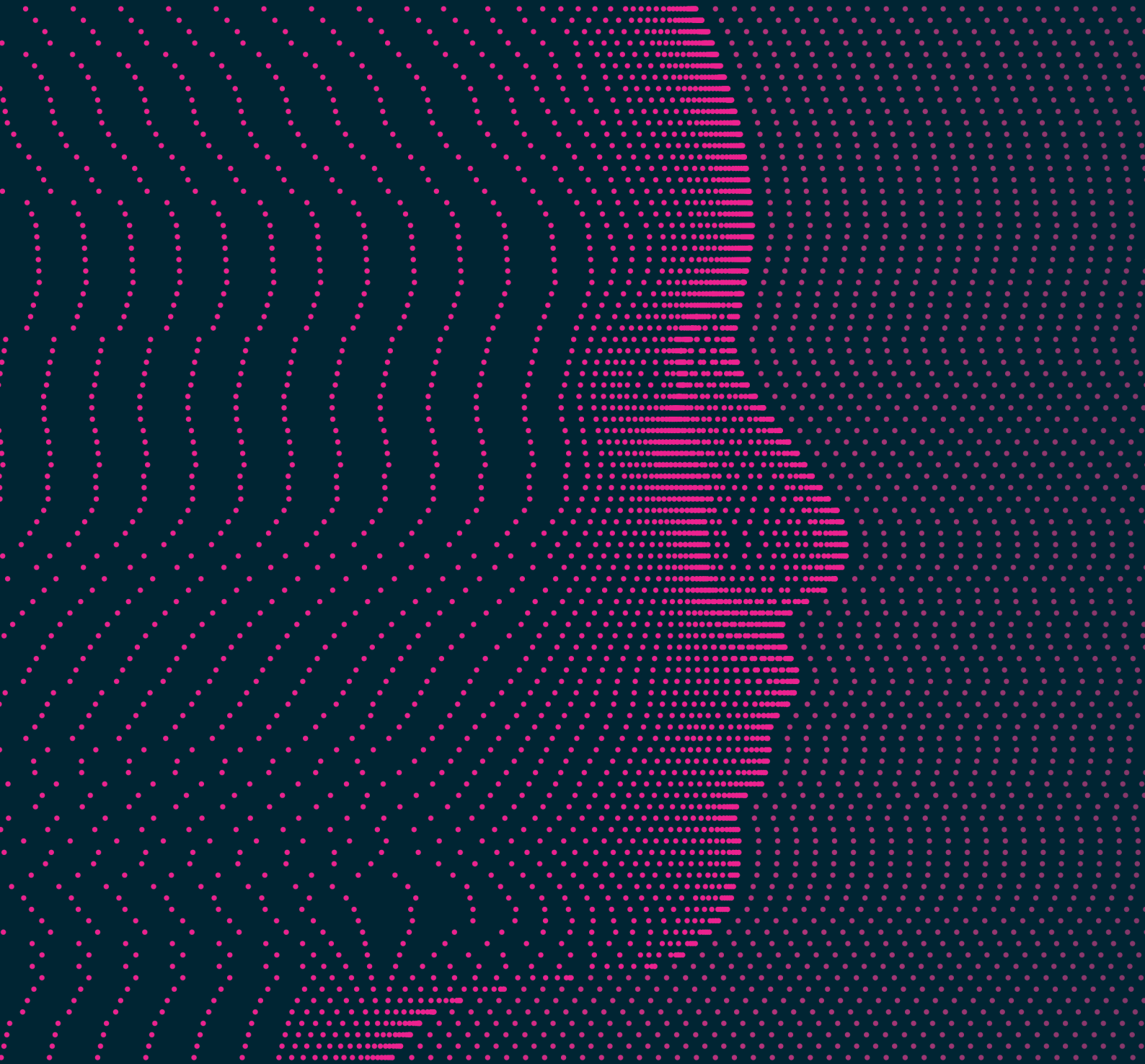


RESHAPING THE FUTURE

Kosovo Women on the Front Line of
Artificial Intelligence and Cybersecurity



RESHAPING THE FUTURE

Kosovo Women on the Front Line of
Artificial Intelligence and Cybersecurity

Authors: Blerta **Thaçi** | Dafina **Olluri**

September, 2024

ABOUT THE PUBLICATION

This publication was prepared within the framework of the **Reshaping the Future: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity** project, funded by **the Embassy of the Netherlands in Kosovo**, and implemented by **IPKO Foundation and Women in Tech Kosovo**. The views expressed in this paper are those of the authors and do not necessarily reflect the positions of **the Embassy of the Netherlands in Kosovo**, or of **IPKO Foundation and Women in Tech Kosovo**.

Acknowledgements

We would like to express our deepest gratitude to **the Embassy of the Netherlands in Kosovo** for their generous support in funding the project **Reshaping the Future: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity**. We extend our appreciation to **IPKO Foundation and Women in Tech Kosovo** for their collaborative efforts in implementing this initiative, which has significantly contributed to the empowerment of women in AI and cybersecurity in Kosovo.

Special thanks go to the trainers, experts, and mentors who dedicated their time and expertise to the success of the workshops and training sessions. Their invaluable guidance and commitment were key in fostering an inclusive environment for women to thrive in these critical fields. We would also like to **acknowledge the women participants**, whose enthusiasm and drive to learn have inspired the core of this report. Their insights and engagement provided vital perspectives that shaped our findings.

Additionally, we thank all **stakeholders and interviewees, including local authorities, NGOs, and professionals**, who contributed their knowledge and experiences, enriching the content of this report.

Table of Contents

List of Acronyms	6
1. Introduction	7
2. Methodology	8
2.1 Secondary Data Analysis	8
2.2 Questionnaire.....	8
2.3 Project Findings	8
2.4 In-depth Interviews.....	8
2.5 Triangulation of Data	8
3. Background and Context	9
3.1 Key Legislative and Strategic Frameworks	9
3.2 Importance of gender diversity in these fields	10
3.3 Historical Roles of Women in Kosovo's Society	12
3.4 Kosovo's Position: AI and Cybersecurity Initiatives in Kosovo	15
3.5 Community-driven Initiatives and Organizations: AI and Cybersecurity Initiatives in Kosovo.....	16
4. Training Summary: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity	19
4.1 Pre-Training Data Insights:.....	19
4.2 Post-Training Data Insights:.....	20
5. Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity	22
6. Recommendations for Ethical and Responsible AI and Cybersecurity Development in Kosovo	27
7. Conclusion	29
7.1 The Future of AI and Cybersecurity in Kosovo: The potential impact of empowering women in these fields.....	29
8. References	30

List of Acronyms

AI	Artificial Intelligence
AKSK	National Authority for Cybersecurity
CICWG	Critical Infrastructure Cybersecurity Working Group
eIDAS	Electronic Identification, Authentication and Trust Services
ENISA	European Union Agency for Cybersecurity
EU	European Union
FSK	Kosovo Security Force
GDPR	General Data Protection Regulation
GIRAI	Global Index on Responsible Artificial Intelligence
ODK	Open Data Kosovo
ICK	Innovation Centre Kosovo
NGO	Non-Governmental Organization
RIT	Rochester Institute of Technology
SMEs	Small and Medium Enterprises
STEM	Science, Technology, Engineering, and Mathematics
UP	University of Prishtina
USAID	United States Agency for International Development

1. Introduction

In the rapidly evolving landscape of artificial intelligence (AI) and cybersecurity, there is a growing global recognition of the need for gender diversity and inclusion. However, in Kosovo, there has been a noticeable absence of initiatives and research focused on women's participation in these fields. With this in mind, the project **"Reshaping the Future: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity,"** funded by the **Embassy of the Netherlands in Kosovo** and implemented by **IPKO Foundation and Women in Tech Kosovo**, sought to address this gap by empowering women through AI and cybersecurity workshops. These workshops were designed not only to provide technical skills but also to encourage women to take on leadership roles in these critical sectors.

More than 50 women from diverse professional backgrounds participated in training, learning to effectively use AI tools and implement cybersecurity measures to protect themselves and their data in the digital space. Beyond the technical training, the initiative aimed to inspire greater representation of women in AI and cybersecurity fields that are traditionally male-dominated. This project became an important step in understanding the broader challenges and opportunities women face in Kosovo's growing tech industry.

Given the lack of comprehensive data and research on women in AI and cybersecurity in Kosovo, this report takes a closer look at global trends in these sectors, highlighting the importance of gender diversity and examining the key legislative and strategic frameworks relevant to Kosovo. The report also explores the historical and cultural context that has shaped the role of women in the country and delves into the current landscape of AI and cybersecurity initiatives in Kosovo. Additionally, with women leading AI and cybersecurity advancements, this initiative is a key step toward creating a more inclusive, secure, and innovative tech environment in Kosovo, promoting equal opportunities and strengthening the country's digital resilience.

2. Methodology

The methodology for this research integrated various approaches thus offering a comprehensive analysis of the challenges and opportunities for Kosovo women in AI and cybersecurity. By using a mixed-method approach, the study ensures a well-rounded understanding of both the quantitative and qualitative aspects of the subject matter.

The methodology encompasses the following key elements:

2.1 Secondary Data Analysis

The research begins with an extensive review of existing literature, reports, and data on AI, cybersecurity, and gender-related issues in Kosovo. Sources include government publications, academic research, NGO reports, and international databases. This secondary analysis helped to establish the foundational context and informed the key areas of inquiry in the study.

2.2 Questionnaire

A structured questionnaire was developed and distributed to women within the community. The survey aimed to gather data on their experiences, challenges, and perspectives regarding gender-based barriers, career opportunities, and security awareness. The responses provided quantitative insights into the current landscape and highlighted key trends relevant to women's participation in these fields.

2.3 Project Findings

This report also incorporates findings from workshops and trainings conducted as part of the project “Reshaping the Future: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity.” These workshops aimed to empower women through hands-on experience with AI tools and enhance their cybersecurity awareness. The practical outcomes of these sessions helped identify areas for further development and support in the field.

2.4 In-depth Interviews

In-depth Interviews were conducted with a range of stakeholders, including women professionals in AI and cybersecurity, local authorities, and representatives from NGOs. These interviews provided qualitative data on personal experiences, systemic barriers, and the specific needs of women entering or working in AI and cybersecurity roles. The insights from these interviews have enriched the analysis with first-hand accounts and contextual depth.

2.5 Triangulation of Data

To ensure the reliability and validity of the research findings, the data gathered from secondary sources, questionnaires, project activities, and interviews were triangulated. This approach helped cross-verify the results and draw more accurate conclusions, leading to actionable recommendations.

Limitations: While the study provides an in-depth look at the role of women in AI and cybersecurity in Kosovo, some limitations exist. The relatively small sample size for the questionnaire and the interviews may not fully represent the broader population. Additionally, as the fields of AI and cybersecurity are still developing in Kosovo, the availability of local data was somewhat limited. Nonetheless, the combination of various research methods provides a balanced and thorough overview of the current landscape.

3. Background and Context

3.1 Key Legislative and Strategic Frameworks

AI and cybersecurity have emerged as two of the most critical and rapidly evolving fields in the global technology landscape. AI, with its ability to automate complex tasks, analyze vast amounts of data, and drive innovation across industries, is reshaping the future of work, business, and daily life. From healthcare and finance to manufacturing and education, AI is being integrated into almost every sector, leading to increased efficiency, cost savings, and the development of entirely new products and services.

A recent study¹ on the **Global Index on Responsible Artificial Intelligence (GIRAI)** ranked Kosovo 109th out of 138 countries, assessing three main pillars: government frameworks, government actions, and non-state actors. The research highlighted that while various AI governance frameworks exist globally, their presence does not necessarily equate to the promotion and advancement of responsible AI. Unlike some countries, Kosovo currently lacks a national AI strategy, which places it at a disadvantage in terms of developing and governing AI responsibly. In many other countries, the national AI strategy often serves as the primary government framework addressing AI, though only 39% of the countries surveyed have such strategies in place.

However, while Kosovo currently does not have a formal AI strategy, we confirmed with the Office of the Prime Minister that there is no existing AI policy in place. Nevertheless, the country compensates for this gap through other significant initiatives in its digital landscape. **The National Cybersecurity Strategy 2023-2027²**, along with documents like the **e-Government Strategy³** and the **Kosovo Digital Agenda 2030⁴**, outlines the government's commitment to digital transformation, which includes plans to integrate AI into future digitalization processes. These frameworks emphasize the importance of cybersecurity and digital governance, laying the foundation for responsible AI integration in the future. **The National Cybersecurity Strategy** focuses on building robust cybersecurity measures to protect against growing digital threats. At the same time, the e-Government Strategy promotes the use of innovative technologies, including AI, to enhance public services.

In addition to these strategic documents, Kosovo has several important laws that provide a solid foundation for managing digital challenges and ensuring a secure online environment as AI continues to develop:

- a. **Law on Personal Data Protection⁵**: This law is pivotal in regulating the processing of personal data and ensuring privacy in the digital age. It aligns Kosovo with European standards, particularly the **General Data Protection Regulation (GDPR)**. As AI technologies increasingly handle sensitive data, this law plays a key role in safeguarding citizens' data and ensuring that AI systems operate responsibly and transparently.

1. Global Index for Responsible AI. Open Data Kosovo, <https://opendatakosovo.org/wp-content/uploads/2024/06/GI-1st-Edition-Report.pdf>.

2. Cybersecurity Strategy 2023-2027. Ministry of Internal Affairs of Kosovo, <https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2692/Strategjia%20p%C3%ABr%20Siguri%20Kibernetike%20-%20ENG..pdf>.

3. e-Government Strategy Kosovo 2023-2027. Ministry of Internal Affairs of Kosovo, <https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf>.

4. Kosovo Digital Agenda 2030. Government of Kosovo, <https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=41846>.

5. Law No. 06/L-082 on Protection of Personal Data. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2>.

- b. **Law on Information Society Services⁶:** This law establishes the legal framework for providing and regulating information society services, including electronic commerce and online contracts. As AI becomes more integrated into digital services, this law is essential in ensuring the secure and lawful operation of AI-powered platforms and services.
- c. **Law on Electronic Identification and Trusted Services in Electronic Transactions⁷:** This law provides the legal basis for secure electronic transactions and trusted services, including electronic identification for authentication purposes. With AI systems increasingly relying on electronic identification for secure access and operations, this law ensures that AI applications can function within a safe and trusted digital environment.

As AI continues to advance, it brings new challenges, particularly in the realm of cybersecurity. The increasing reliance on digital systems and AI technologies has made cyber threats more sophisticated and widespread. Cybersecurity has become a top priority for governments, businesses, and individuals alike, as the risk of data breaches, cyberattacks, and other digital threats grows. The interconnectedness of global systems means that a security breach in one area can have far-reaching consequences, underscoring the need for robust cybersecurity measures. **“According to the Deputy Director General of the Information Society Agency, the Agency is actively engaged in raising cybersecurity awareness through various initiatives. These efforts include educating government employees on safe digital practices, such as the responsible use of webmail on personal devices, and enforcing a ban on the use of USB devices within government infrastructure.”⁸**

AI is also playing a dual role in cybersecurity—both as a tool to enhance security measures and as a target for new types of attacks. Machine learning algorithms, for example, are being used to detect anomalies and prevent attacks, while adversarial AI techniques are being developed to exploit vulnerabilities in these systems. This ongoing arms race between attackers and defenders in the cyber domain makes it crucial to stay ahead of emerging threats.

3.2 Importance of gender diversity in these fields

Despite the significant advances in AI and cybersecurity, these fields have historically been dominated by men, leading to a lack of diversity that can limit innovation and effectiveness. Gender diversity is not just a matter of social equity; it is a critical factor in creating more robust, inclusive, and innovative technologies. Diverse teams bring different perspectives, experiences, and problem-solving approaches, which are essential for tackling the complex challenges posed by AI and cybersecurity.

In AI, for example, the lack of gender diversity has been linked to biases in algorithms, which can perpetuate stereotypes and exclude or disadvantage certain groups. Ensuring that women are actively involved in the development and deployment of AI systems is crucial for creating technologies that are fair, ethical, and representative of the diverse populations they serve.

6. Law No. 04/L-094 on the Information Society Services. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811&langid=2>.

7. Law No. 08/L-022 on Electronic Identification and Trust Services in Electronic Transactions. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=51618&langid=2>.

8. Hamzaj, Genc. Interview. Conducted by Blerta Thaçi and Dafina Olluri, 25 Sept. 2024. Information Society Agency, <https://ashi-upi.rks-gov.net/en>.

Similarly, in cybersecurity, diverse teams are better equipped to understand and address the wide range of threats that exist in the digital world. Women bring unique insights into how different communities and individuals interact with technology, which can inform more effective security strategies. Moreover, as cyber threats increasingly target personal data and privacy, having women involved in cybersecurity efforts ensures that these concerns are addressed from multiple angles.

The push for gender diversity in AI and cybersecurity is gaining momentum globally, with initiatives aimed at increasing the representation of women in these fields. Organizations, governments, and educational institutions are recognizing the need to create more inclusive environments that support women in tech, from providing STEM education and training opportunities to promoting women into leadership roles.

Around the world, technology-facilitated gender-based violence is increasingly recognized as a pervasive issue. This form of violence spans from cyberstalking and online harassment to the non-consensual distribution of explicit images, disproportionately affecting women and marginalized groups.

One stark example is the “**Albkings**” case in Kosovo, where a Telegram group of over 100,000 members engaged in sharing personal and explicit information about women without their consent. The group’s activities reflect broader global trends where patriarchal norms are reinforced and amplified by digital platforms. This case illustrates the complex intersection of technology, gender, and violence, highlighting the need for robust global and local responses.

Globally, such incidents underscore the urgent need to address the gaps in legal frameworks, improve technological safeguards, and promote cultural shifts that recognize and combat online misogyny. While digital platforms have democratized access to information and expression, they have also created new arenas for the perpetuation of gender-based violence, making it imperative for policymakers, tech companies, and civil society to collaborate on solutions.

The Albkings case is particularly significant in the context of Kosovo, a country still grappling with its post-conflict identity and gender norms, but it also resonates with similar issues faced by women worldwide. The global community must recognize that these are not isolated incidents but rather part of a larger pattern of technology being used as a tool for both empowerment and oppression. Additionally, an interview was conducted with Ms. **Xhorxhina Bami**, a statement correspondent for **Kosovo at Balkan Insight** and **Editor at Prishtina Insight**. One specific aspect discussed was how, based on her work, she perceives the portrayal of women and girls on the internet through AI tools in Kosovo, possibly linking this to the Albkings case.

While AI can be harnessed for numerous positive developments, its unregulated nature and novelty have led to its misuse, particularly in violating the rights of society’s most vulnerable groups, including women, children, and queer individuals. The absence of specific internet regulations in Kosovo has created a legal vacuum, making it difficult for authorities to effectively protect users from online abuse. In Kosovo, as in other Balkan countries, online gender-based violence is not criminalized. For instance, acts like slut-shaming should be addressed under other criminal offenses such as hate speech, harassment, or the unauthorized distribution of someone else’s photos, unauthorized photography, and recording, Ms. **Xhorxhina Bami** said.

9. Kosovo Law Ignores Tech-Facilitated Abuse of Women, BIRN Report.” Balkan Insight, 25 June 2024, <https://balkaninsight.com/2024/06/25/kosovo-law-ignores-tech-facilitated-abuse-of-women-birn-report/>.

In a study¹⁰ published in **Balkan Insight in March of 2024**, Ms. Bami analyzed 427 TikTok videos targeting girls and women, labeling them as immoral. One TikTok account, identified during the investigation, had posted 142 videos with over 8 million views, abusing women and girls from Kosovo. These videos or photos featured girls and women in normal situations, but with offensive descriptions. One of the girls, who along with her friends was targeted by this account, reported that they had tried to seek help from the police several times, but were told that the police could not identify the person behind the account due to the inability to trace the IP address.

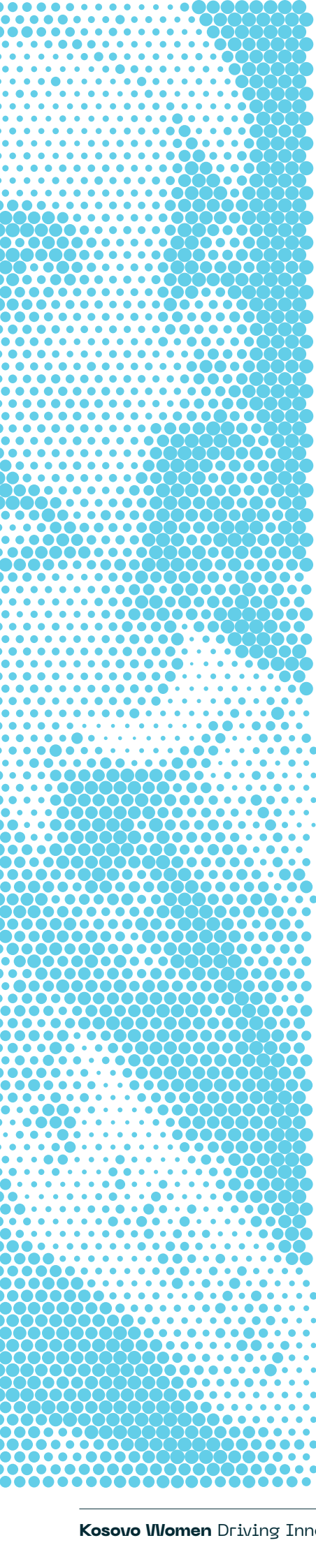
Some of the posts identified on TikTok were also shared in the Albking's group, where seven people were arrested in May, and one more in February 2023 following a report by a girl. On Telegram, authorities have managed to identify some individuals who have been arrested, while the investigations are ongoing. However, other social networks enable greater anonymity, making it more challenging to trace perpetrators. In the Albking's group, alongside videos and photos of women and girls stolen from their social media profiles or shared without consent, there have been instances of AI modifications, deep fake images, and the sharing of personal information such as phone numbers and identification. Many videos on TikTok and other social networks, as well as information shared in the Albking's group on Telegram, have included offers for paid intimate relations with girls and women without their knowledge.

3.3 Historical Roles of Women in Kosovo's Society

Throughout history, women in Kosovo have held significant roles within the household and community, but these roles were largely confined to the private, domestic sphere, deeply influenced by traditional customs such as the **Kanun of Lekë Dukagjini**¹¹, a set of customary laws that governed Albanian society. The Kanun reinforced strict patriarchal structures, defining women's responsibilities largely around family care and household duties while excluding them from political, economic, and legal decision-making processes. Women were expected to maintain the household, raise children, and uphold family honor, while men controlled land ownership, political power, and leadership positions. The education of girls was often limited, further restricting their opportunities outside the domestic realm.

10. "TikTok Used Across Balkans to Slutshame Women and Girls." *Balkan Insight*, 6 Mar. 2024, <https://balkaninsight.com/2024/03/06/tiktok-used-across-balkans-to-slutshame-women-and-girls/#:~:text=A%20BIRN%20analysis%20of%20hundreds,sexual%20behaviour%20%2D%20'slutshaming>.

11. "Code of Lekë Dukagjini." *Wikipedia*, https://en.wikipedia.org/wiki/Code_of_Lek%C3%AB_Dukagjini.



Despite these limitations, women in rural communities played crucial roles in maintaining agricultural economies, working in fields alongside men and contributing to the family's livelihood. Their labor, while significant, was rarely acknowledged in formal terms, reinforcing their subordinate status.

Post-independence shifts brought significant changes. Kosovo's transition to democracy and its alignment with European norms created new opportunities for women, particularly in education, politics, and the workforce. Gender quotas were introduced in parliamentary elections, leading to increased women representation in government. Women also began to enter professions previously dominated by men, including law, medicine, and business. **The Constitution of Kosovo (2008)** formally guarantees gender equality, and legislation such as the **Law on Gender Equality**¹² aims to eliminate discrimination and promote equal opportunities for women in public and private life.

However, despite these legal advancements, traditional patriarchal values remain deeply rooted in some parts of society. Women continue to face social and institutional barriers, including unequal access to leadership roles, wage gaps, and gender-based violence. In many rural areas, traditional views about women's roles persist, limiting their participation in public life and access to education and employment opportunities. Furthermore, cultural expectations often place the burden of caregiving and household duties on women, even as they pursue careers outside the home.

Women's movements and civil society organizations have been instrumental in advocating for gender equality, challenging traditional norms, and pushing for further reforms. These efforts have led to increased awareness and gradual changes in societal attitudes, though much work remains to be done to achieve full gender equality in Kosovo.

Formal higher education in Kosovo began with the establishment of the **University of Prishtina** in the 1969/70 academic year. Initially, the representation of women in engineering was low, but it has steadily increased, reaching 61.8% in the 2020/2021 cohort. This progress highlights a significant transformation toward gender balance in engineering fields.

Women are significantly reshaping the tech landscape of Kosovo. Several notable figures have blazed trails in engineering and technology, serving as inspirations for future generations of women in these fields. Their contributions have not only broken gender barriers but also continue to pave the way for young girls to pursue careers in engineering and technology.

12 . Kosovo Assembly Official Website. <http://old.kuvendikosoves.org/?cid=2,191,103>.

Myzafere Limani¹³, one of the first woman engineers in Kosovo, became the first woman to hold a professorship at the **Faculty of Electrical Engineering**. As a member of the **Kosovo Academy of Sciences**, she remains a role model and source of inspiration for young girls pursuing engineering careers.

Vjollca Komoni¹⁴, another early pioneer in the engineering field, has made significant contributions as a professor in the energy sector. She has dedicated her career to empowering and inspiring young women to enter and thrive in engineering disciplines.

Teuta Sahatqija¹⁵, a notable figure in Kosovo's tech sector, began her career as a commercial software programmer in 1985, making her the **first woman programmer** in the country. Her early work in software development helped pave the way for more women in technology, and she continues to be a strong advocate for gender equality in tech to this day.

Gentiana Alija Shala¹⁶, a trailblazer in solar energy, stands out as the founder and CEO of the only woman-led solar energy company in Kosovo. Her company, which employs an all-women engineering team, has successfully implemented projects in numerous countries. Shala's ambition and creativity have allowed her to defy gender expectations and establish herself as a leader in a male-dominated industry.

Since then, the educational landscape in Kosovo has been evolving, with an increasing number of women accessing higher education, including STEM fields. Despite this progress, significant challenges persist. Traditional gender roles and socio-cultural expectations continue to discourage women from pursuing careers in these areas, contributing to a gender gap in STEM education and professions.

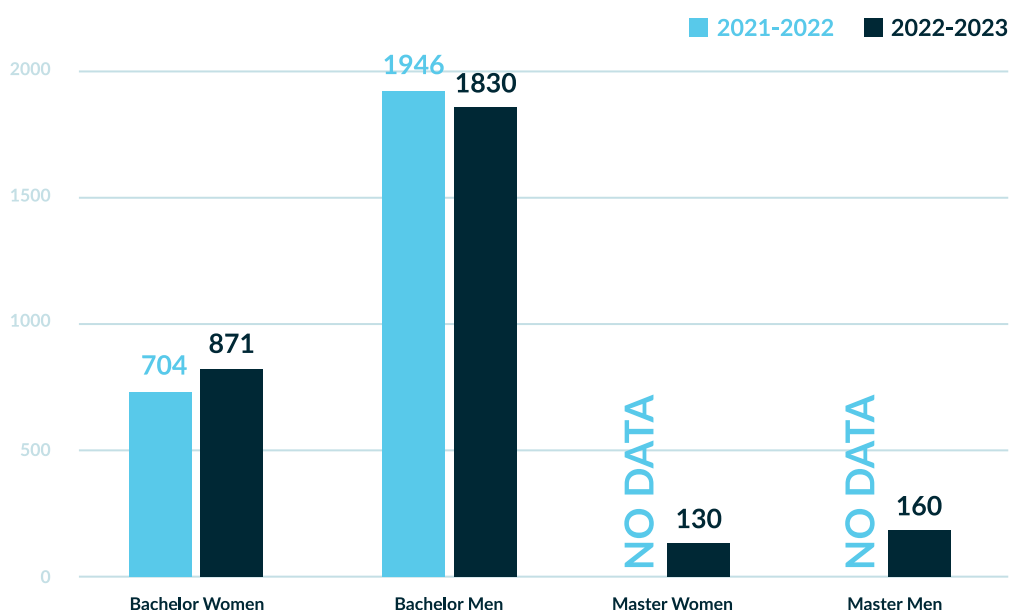


Figure 1. The number of students enrolled in Higher Education -Information and Communication Technology (Bachelor & Master for the years 2021/2022 and 2022/2023), Data Source: Agency of Statistics of Kosovo

13. Limani, Myzafere. Akademia e Shkencave dhe e Arteve e Kosovës, <https://ashak.org/anetaret/myzafere-limani/#:~:text=Biografia.%20Myzafere%20Krasniqi-Limani%20e%20lindur%20n%C3%AB%20Pej%C3%AB%20m%C3%AB>.

14. Komoni, Vjollca. Professor of Electrical Engineering, University of Prishtina. Google Scholar, https://scholar.google.com/citations?user=7hz_5LoAAAAJ#:~:text=Articles%20%E2%80%93%20%E2%80%AAProfessor%20of%20Electrical%20Engineering,%20University%20of.

15. Sahatqija, Teuta. "Success Story: Women in Tech." TACSO, <https://tacso.eu/story/success-story-women-in-tech/>

16. Alija Shala, Gentiana. "A Sustainable Future Comes from Women Changemakers." UNDP Eurasia, <https://www.undp.org/eurasia/stories/sustainable-future-comes-women-changemakers#:~:text=Gentiana%20Alija%20Shala%20is%20a%20solar%20energy%20engineer>.

However, the analysis presented in Figure 1 from the report “Sector Overview of the ICT Sector,” which examines the number of students enrolled and graduated in University Education for Information and Communication Technology, reveals a positive trend: women enrollment in bachelor’s programs has increased, while men enrollment has seen a slight decline. This indicates a promising shift toward greater female participation in STEAM-related fields.

3.4 Kosovo’s Position: AI and Cybersecurity Initiatives in Kosovo

While Kosovo has shown interest in advancing in the fields of AI and cybersecurity, it currently lacks significant national initiatives, strategic frameworks, and active involvement from key organizations. The landscape of AI and cybersecurity in Kosovo is still in its early stages, with limited integration of these technologies into sectors such as education, public administration, and private enterprises.

However, there are a few non-state actors in Kosovo who have taken the initiative to focus on AI and cybersecurity, either as standalone areas or as part of a broader range of services. These initiatives, though limited in number, play a crucial role in integrating AI and cybersecurity into the local landscape.

Some organizations are offering specialized training programs for their staff and the broader community, aimed at enhancing skills in these emerging fields. Others are actively incorporating AI and cybersecurity tools into their existing systems to improve efficiency and security. These efforts, while still in their early stages, demonstrate the growing recognition of the importance of AI and cybersecurity in Kosovo’s development, even in the absence of a comprehensive national framework.

Kosovo has seen the development of educational programs and research initiatives aimed at fostering a new generation of professionals skilled in AI and cybersecurity. Universities and institutions are offering courses in AI and data science, preparing students for the challenges of digital transformation. These programs are critical in addressing the skills gap and ensuring that Kosovo can meet the demands of a rapidly evolving digital economy.¹⁷

Kosovo’s efforts in AI and cybersecurity are bolstered by international cooperation, particularly through alignment with European standards such as the GDPR and the Budapest Convention on Cybercrime. These collaborations help Kosovo stay up-to-date with global best practices in cybersecurity and AI governance, enhancing the country’s ability to protect its digital infrastructure.

17 . Implications of AI Adoption on Kosovo’s Tech SMEs. Rochester Institute of Technology, n.d., Thesis. RIT Scholar Works, <https://repository.rit.edu/cgi/viewcontent.cgi?article=12972&context=theses>

3.5 Community-driven Initiatives and Organizations: AI and Cybersecurity Initiatives in Kosovo

Kosovo is slowly emerging as a hub for innovation in both AI and cybersecurity, with a growing number of key players and organizations actively contributing to the digital transformation of the country. These initiatives are driven by a collective effort to enhance technological capabilities, safeguard critical infrastructure, and empower future generations with advanced digital skills. Institutions like the National Authority for Cybersecurity (AKSK), Cyber Kosovo Team, the Innovation Centre Kosovo (ICK), and initiatives backed by international partners such as United States Agency for International Development (USAID) are playing a pivotal role in promoting cybersecurity resilience. At the same time, organizations such as the IPKO Foundation, Women in Tech Kosovo, AI Kosovo and Open Data Kosovo are advancing AI research, focusing on building responsible AI solutions to address societal challenges. Together, these players are helping Kosovo position itself as a leader in digital innovation and security in the Western Balkans.

- d. **Cyber Fortress 2024**¹⁸: This is a simulation-based cybersecurity event organized by Kosovo's National Authority for Cybersecurity (AKSK), in collaboration with international partners like CRDF Global and supported by the U.S. Department of State. The event involved cybersecurity experts from Kosovo and Albania participating in competitive, scenario-based simulations designed to address and solve cyber incidents. This initiative helps to strengthen the capabilities of cybersecurity professionals while promoting international cooperation.
- e. **FIEK – University of Prishtina (UP)** has been at the forefront of cybersecurity initiatives, playing a crucial role in advancing knowledge and skills in this critical field. Since 2017, FIEK has organized the annual Conference on Privacy and Security¹⁹, providing a platform for experts, academics, and professionals to discuss and address the evolving challenges of privacy and cybersecurity. Additionally, FIEK has actively collaborated with international partners, most notably in the Cyber Defense Competition (CDC)²⁰, held in partnership with Iowa State University, the Kosovo Security Force (FSK), and the Iowa National Guard. FIEK secured first place in 2022 and second place in both 2023 and 2024, and the university is already preparing for participation in 2025. FIEK is also a key contributor to BSides Prishtina, having hosted and actively participated in the event in 2022, 2023, and 2024, bringing global cybersecurity discussions and hands-on workshops to the local community. The university is a strong advocate for increasing diversity in the field, supporting initiatives such as Girls in Cyber²¹, which focuses on empowering young women through education, mentorship, and engagement in cybersecurity. Furthermore, FIEK is backing the Kosovo Cyber Team²² in their participation in the European Cybersecurity Challenge 2024²³, hosted by ENISA²⁴. This marks Kosovo's first involvement in the prestigious competition, reflecting FIEK's commitment to elevating Kosovo's presence on the European cybersecurity stage.

18. "AKSK Organizes 'Cyber Fortress 2024': A Digital Battle for Cybersecurity Experts from Albania and Kosovo." Albania Tech, 25 July 2024, <https://albaniatech.org/aksk-organizes-cyber-fortress-2024-a-digital-battle-for-cybersecurity-experts-from-albania-and-kosovo/>.

19. "Conference on Privacy and Security." Facebook, <https://www.facebook.com/share/p/eGy7n9BgWHRGAVvy/>.

20. "Cyber Defense Competition." LinkedIn, https://www.linkedin.com/posts/blera_iowa-kosova-fsk-activi-ty-6932957138457657344-pPVD/.

21. "Girls in Cyber." Facebook, <https://www.facebook.com/share/p/nqhaFhddpTjEuXuP/>.

22. Kosovo Cyber Team. <https://kosovacyber.team/>.

23. European Cybersecurity Challenge 2024. LinkedIn, <https://www.linkedin.com/company/ecsc2024/>.

24. European Union Agency for Cybersecurity (ENISA) – European Cybersecurity Challenge 2024. <https://ecsc2024.it/>.

- f. **BSides Prishtina**²⁵ is an exciting new initiative aimed at fostering a stronger cybersecurity community in Kosovo. As part of the global BSides movement, this event will bring together cybersecurity professionals, enthusiasts, and experts to share knowledge, explore the latest trends, and collaborate on innovative solutions. Through talks, workshops, and hands-on activities, BSides Prishtina seeks to empower local talent, promote cybersecurity awareness, and create a platform for meaningful dialogue and skill development in the field.
- g. **Kosovo Critical Infrastructure Cybersecurity Working Group (CICWG)**²⁶: Supported by USAID, this multi-stakeholder initiative brings together public and private sector representatives to address cybersecurity challenges related to critical infrastructure. The group played a significant role in drafting Kosovo's first comprehensive cybersecurity law and continues to advise the government on implementing best practices and policy frameworks.
- h. **Innovation Centre Kosovo (ICK)**²⁷: ICK runs an advanced cybersecurity training program that offers a hands-on approach to both offensive and defensive cybersecurity strategies. Participants are trained through real-life scenarios on defending and attacking digital infrastructures. The program is designed to build a new generation of cybersecurity experts by teaching them both technical skills and policy awareness. This initiative is particularly relevant for young professionals looking to build careers in cybersecurity.
- i. **RIT Kosovo Cybersecurity Exercises**²⁸: RIT Kosovo actively participates in international cybersecurity competitions and hackathons, such as the Cyber Security Defense Competition (CSDC), which brings students and experts together to solve complex cybersecurity challenges. These events help foster global talent and innovative approaches to cybersecurity solutions.
- j. **Women4Cyber Kosovo**: is an initiative aimed at increasing female participation in the cybersecurity sector in Kosovo. It operates under the broader Women4Cyber Europe network, which strives to bridge the gender gap in cybersecurity by providing training, mentorship, and networking opportunities for women. The organization focuses on capacity building, education, and empowering women through specialized programs designed to enhance their cybersecurity skills and create opportunities in both the public and private sectors.

25 . BSides Prishtina. <https://bsidesprishtina.org/>.

26 . Berisha, Albulena Xhelili, and Inta Plostins. "How Multi-Stakeholder Coalitions Can Enhance Policy and Regulatory Frameworks for Cybersecurity." DAI Global Digital, 25 Apr. 2024, <https://dai-global-digital.com/how-multi-stakeholder-coalitions-can-enhance-policy-and-regulatory-frameworks-for-cybersecurity.html>.

27 . "Cyber Unity: Cyber Security Training." Innovation Centre Kosovo, <https://ickosovo.com/training/courses/cyber-unity-cyber-security-training1>.

28 . "RIT K Students in International Cybersecurity Exercise 2024." RIT Kosovo, 26 Feb. 2024, <https://www.rit.edu/kosovo/news/rit-k-students-international-cybersecurity-exercise-2024>.

- k. **AI Kosovo** - is a community-driven initiative founded in 2021 with the goal of expanding and supporting the development and adoption of AI technologies in Kosovo. Initially focused on general AI information sessions, the community has since evolved to include more technical discussions, particularly around the mathematics and programming of neural networks. AI Kosovo now boasts a vibrant community of over 120 participants, ranging in age from 14 to 45, and representing a wide array of professional backgrounds, including software engineers, researchers, CEOs, game developers, and students. Through collaboration with local and international partners, AI Kosovo promotes AI education, research, and innovation. The organization hosts workshops, technical sessions, and events, providing opportunities for knowledge sharing and networking among professionals and enthusiasts alike. By fostering a diverse and engaged community, AI Kosovo plays a pivotal role in shaping the future of AI in the region.
- l. **The Global Index on Responsible AI (GIRAI)** is a flagship project by the Global Center on AI Governance, aimed at tracking and measuring countries' commitments and progress towards responsible AI. Open Data Kosovo is participating in the research focused on Kosovo, contributing to the data collection and analysis that helps provide a comprehensive understanding of how nations are addressing the ethical, social, and regulatory challenges posed by AI technologies.
- m. **Women in Tech Kosovo** - Established in 2021, Women in Tech Kosovo is one of the 60 chapters of the global Women in Tech (WiT) movement. WiT aims to empower 5 million women and girls worldwide by focusing on education, business skills, advocacy, and digital inclusion. With a global community of 250,000 members, WiT organizes an annual Global Summit in Paris and hosts award ceremonies across the world to celebrate achievements in technology. Women in Tech Kosovo have been represented at these prestigious events by notable figures, including President Vjosa Osmani in 2022, Former President Atifete Jahjaga, and Chapter Ambassador Teuta Sahatqija. Kosovo has consistently had nominees and awardees in the European Women in Tech Awards, with recognition in categories such as Lifetime Achievement, Aspiring Teens, and Most Impactful Initiative. In 2024, three young women who excelled in an Artificial Intelligence training program, part of the MATRA project co-organized by IPKO Foundation and Women in Tech Kosovo, were honored with the opportunity to attend the Women in Tech Global Summit in Paris. Over 100 Kosovars, primarily women and girls, have pursued master's degrees or university courses through the European Business University in Luxembourg, a partner of Women in Tech. These opportunities were offered at a symbolic cost. They included advanced courses in Artificial Intelligence, Machine Learning, Python Programming, and other cutting-edge technologies, significantly enhancing their knowledge in high-tech and AI fields. Women in Tech Kosovo has organized numerous conferences and workshops on Cyber Security and Artificial Intelligence and its applications. These events, featuring distinguished speakers, have targeted students, women in agriculture and business, and women from vulnerable communities, fostering cross-country collaborations and connecting Kosovo's women to the global Women in Tech network.

4. Training Summary: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity

As part of the project “Reshaping the Future: Kosovo Women on the Front Line of Artificial Intelligence and Cybersecurity,” funded by the Embassy of the Netherlands in Kosovo, implemented by IPKO Foundation and Women in Tech Kosovo, a significant initiative was undertaken to empower women in the tech industry. More than 50 women from various backgrounds participated in AI workshops designed to equip them with the skills to use AI tools effectively and to stay protected in the digital landscape. These workshops were not just about technical training; they aimed to inspire and enable women to take leadership roles in AI and cybersecurity in Kosovo. The participants were introduced to cutting-edge AI technologies and learned how to implement these tools in their professional environments while also focusing on cybersecurity measures to ensure their safety and the safety of their data.

4.1 Pre-Training Data Insights:

The pre-training data insights in Figure 2. provide a snapshot of participants’ online behavior and initial cybersecurity awareness. The data reveals high engagement with social media platforms, a tendency to share personal information online, and a significant amount of time spent on the internet daily. These behaviors expose participants to potential cybersecurity risks, which were further emphasized by their experiences with unknown contacts online.

Additionally, while some participants had a basic understanding of cybersecurity terms, there was confusion between concepts like “cyberstalking” and “cyberbullying,” indicating the need for clearer education on these threats.

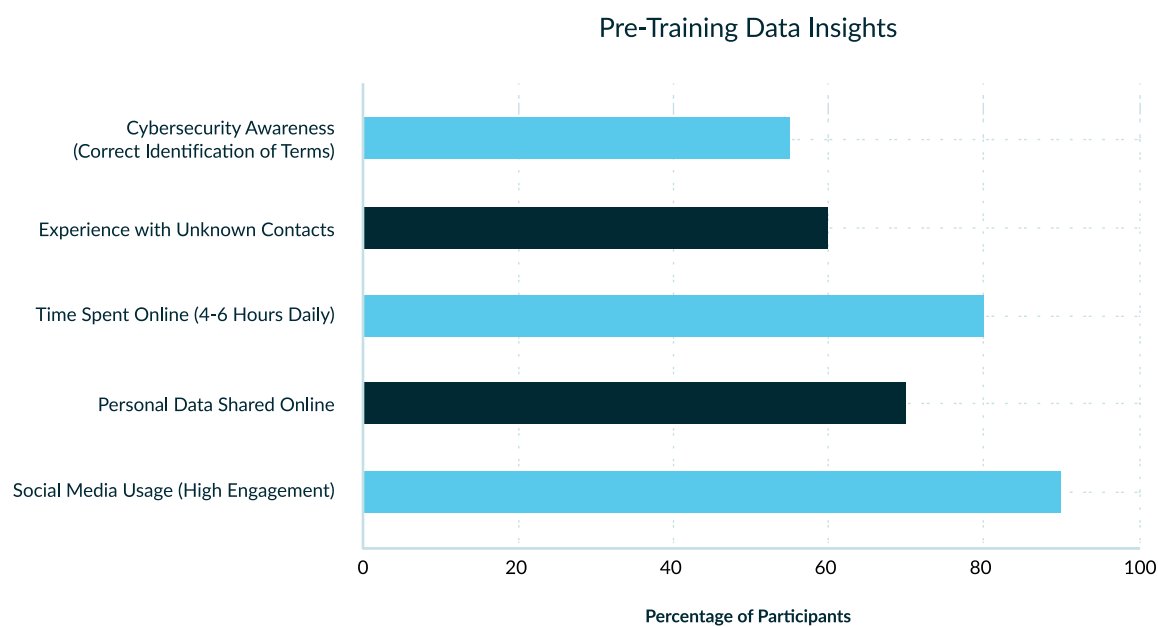


Figure 2. Pre-training data insights Data Source: IPKO Foundation and Women in Tech Kosovo

- a. **Social Media Usage:** The participants commonly used social media platforms such as Instagram, TikTok, and Snapchat, with multiple selections per participant, indicating high engagement with these platforms.
- b. **Personal Data Shared Online:** Many participants shared personal information, such as their full name, date of birth, personal photos, and location, online. This suggests a potential vulnerability in terms of data privacy and awareness about the risks of sharing personal information.
- c. **Time Spent Online:** A significant portion of participants reported spending 4-6 hours online daily, with some even spending up to 12 hours. This high online presence increases their exposure to potential cybersecurity threats.
- d. **Experience with Unknown Contacts:** Several participants indicated they had been contacted by unknown individuals online, pointing to a risk of encountering phishing attempts or other forms of cyber harassment.
- e. **Cybersecurity Awareness:** When asked about terms like “cyberstalking,” most participants correctly identified it, but some confused it with other terms like “cyberbullying,” indicating a need for a clearer understanding of different cybersecurity threats.

4.2 Post-Training Data Insights:

The post-training data insights reflect the positive impact of the cybersecurity workshops on participants. After the training, most participants rated the training environment and content highly, indicating satisfaction with the program.

The trainers received excellent evaluations, and there was a marked improvement in participants’ understanding of key cybersecurity concepts, such as distinguishing between “cyberstalking” and “cyberbullying.” Moreover, the training helped participants recognize the importance of protecting their personal information on social media, leading to a more informed and cautious approach to their online activities.

These insights demonstrate the effectiveness of the training in enhancing cybersecurity awareness and reducing vulnerabilities.

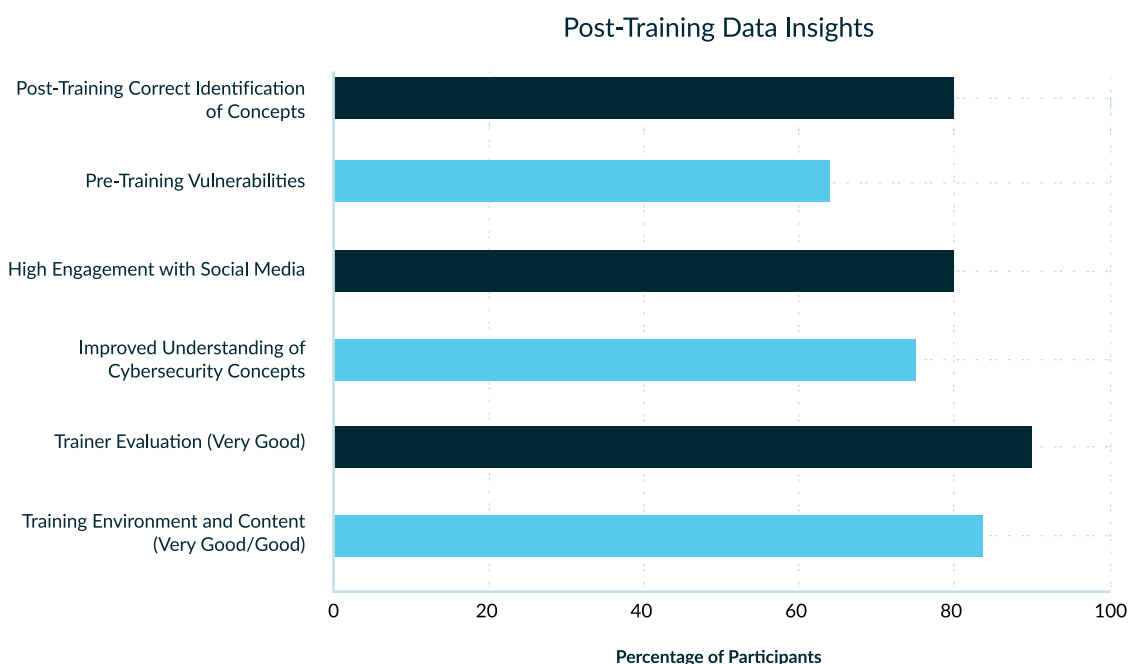


Figure 3. Post-training data insights Data Source: IPKO Foundation and Women in Tech Kosovo

- a. **Training Environment and Content:** The majority of participants rated the training environment and content as “very good” or “good,” indicating satisfaction with the training’s delivery and relevance.
- b. **Trainer Evaluation:** The trainers received positive feedback, with most participants rating their performance as “very good.” This suggests that the trainers were effective in conveying the material.
- c. **Change in Awareness:** There was a noticeable improvement in understanding specific cybersecurity concepts post-training, such as distinguishing between “cyberstalking” and “cyberbullying.” This indicates that the training effectively clarified these concepts.
- d. **High Engagement with Social Media:** The participants are highly active on social media, which underscores the importance of cybersecurity training focused on protecting personal information and recognizing online threats.
- e. **Pre-Training Vulnerabilities:** Before the training, many participants shared sensitive personal data online and spent considerable time on the internet, increasing their risk of exposure to cyber threats.
- f. **Positive Impact of Training:** The training workshops significantly improved participants’ understanding of key cybersecurity concepts, as evidenced by their ability to correctly identify terms and concepts post-training.

5. Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity

In the framework of this initiative an assessment was conducted to capture insights from 121 respondents who participated in AI and cybersecurity workshops. This assessment, consisting of 10 questions, provides valuable insights into the current landscape of women's engagement with AI tools, cybersecurity awareness, and the need for more inclusive policies in Kosovo's tech industry.

The findings reveal that 57.4% of participants were in the age group 18-24 years old, and geographically, 32% were from Prishtina, 15.6% from Lipjan, and 6.6% from Gjilan. While many women in Kosovo are engaging with AI tools and recognize the importance of cybersecurity, there are significant gaps in training and formal education. Participants expressed a clear need for policy interventions, awareness campaigns, and increased funding to protect women online and empower them to take leadership roles in the tech industry.

- a. In response to the question “Select all artificial intelligence (AI) tools that you are familiar with or use regularly?” ChatGPT stood out as the most widely recognized, with 95.9% of participants indicating they are familiar with or use it regularly. This underscores ChatGPT’s role as a leading tool for everyday tasks and problem-solving. Canva, known for its AI-driven design capabilities, followed with 57.4%, reflecting its importance in creative fields like visual content creation and digital marketing. Gemini was familiar to 27% of participants, indicating a growing interest in more advanced AI tools among a segment of women. These results suggest that while widely used, accessible AI tools are popular, there is a rising curiosity about more specialized technologies among women in Kosovo.

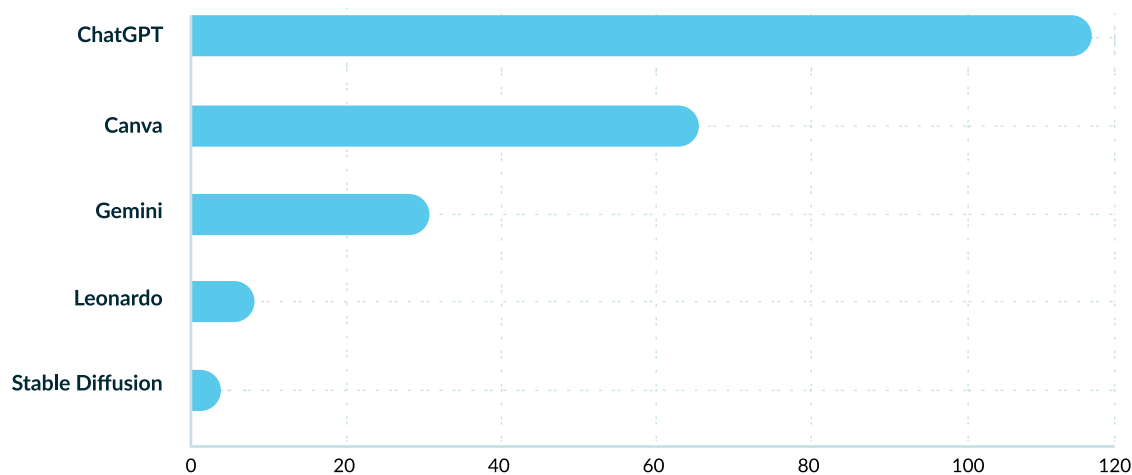


Figure 4. Select all artificial intelligence (AI) tools that you are familiar with or use regularly? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- b. Addressing the question “Have you ever attended any Cybersecurity or Artificial Intelligence training?” 55.7% of participants answered yes, citing a variety of training sources, including private training centers and community-based organizations. This reflects a growing local effort to introduce women to these critical fields through structured programs. For the 44.3% who responded no, many chose to educate themselves through online courses and other digital resources, highlighting the importance of accessible online learning. These findings indicate a mix of formal and self-driven education pathways, underscoring the need for more targeted training opportunities to close the knowledge gap.

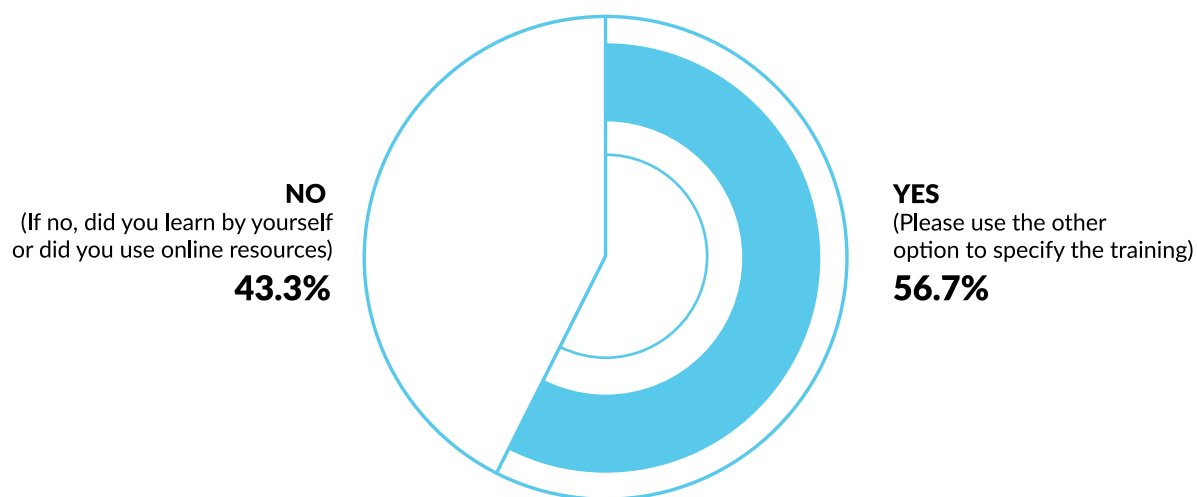


Figure 5. Have you ever attended any Cybersecurity or Artificial Intelligence training? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- c. Concerning the question “On a scale of 1 to 5, how would you rate your current digital skills? (1 = Beginner, 5 = Expert),” 46.7% of participants rated themselves at a 3, indicating moderate digital proficiency. 27% rated their skills at a 4, while 13.9% considered themselves experts with a rating of 5. These results suggest that most women see themselves as having intermediate digital skills, with a smaller portion feeling highly confident in their expertise, highlighting an opportunity for further skill development.

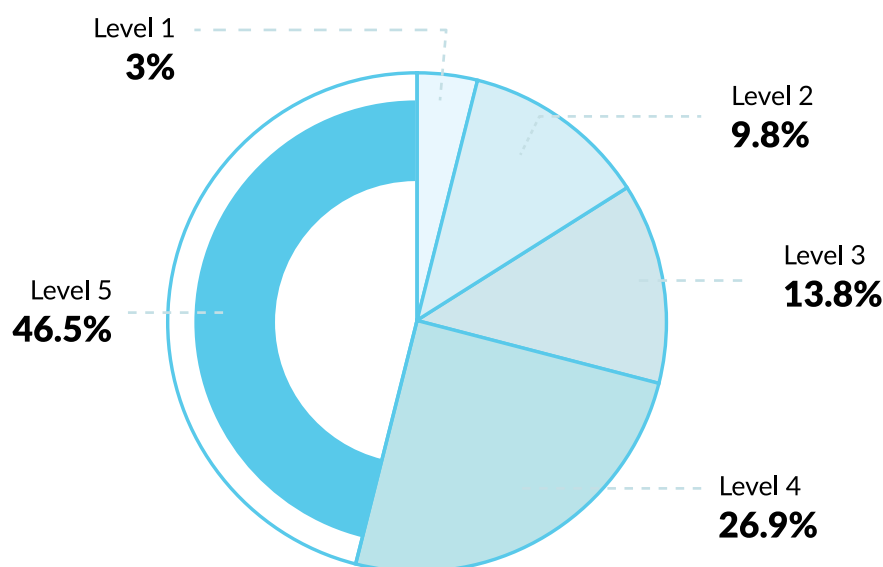


Figure 6. On a scale of 1 to 5, how would you rate your current digital skills? (1 = Beginner, 5 = Expert)? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- d. In response to the question “How safe do you feel in the digital world?” 48.4% of participants said they feel somewhat safe, while 37.7% responded mostly safe, and 9.8% indicated they feel not safe. These results suggest that while many women feel relatively secure online, a significant portion still harbors concern about their digital safety, highlighting the need for improved cybersecurity education and protections.

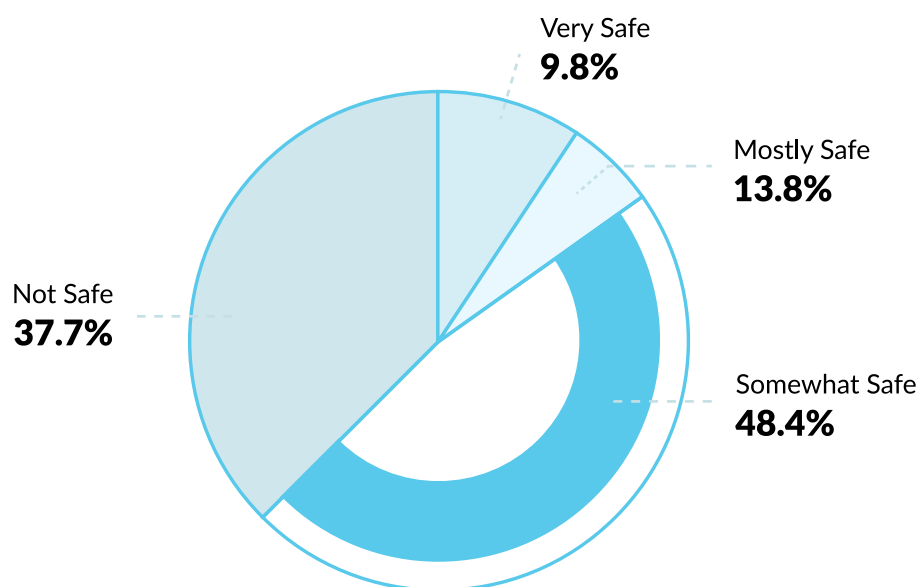


Figure 7. How safe do you feel in the digital world? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- e. In response to the question “In your opinion, what are the most serious cybersecurity threats women face online today?” 81.1% of participants identified online bullying and cyberbullying as a major threat. 72.1% highlighted identity theft, while 64.8% pointed to revenge porn and the non-consensual sharing of intimate images. These findings underscore the prevalence of both personal and privacy-related threats that women face online, reinforcing the need for stronger protections and awareness around digital security for women.

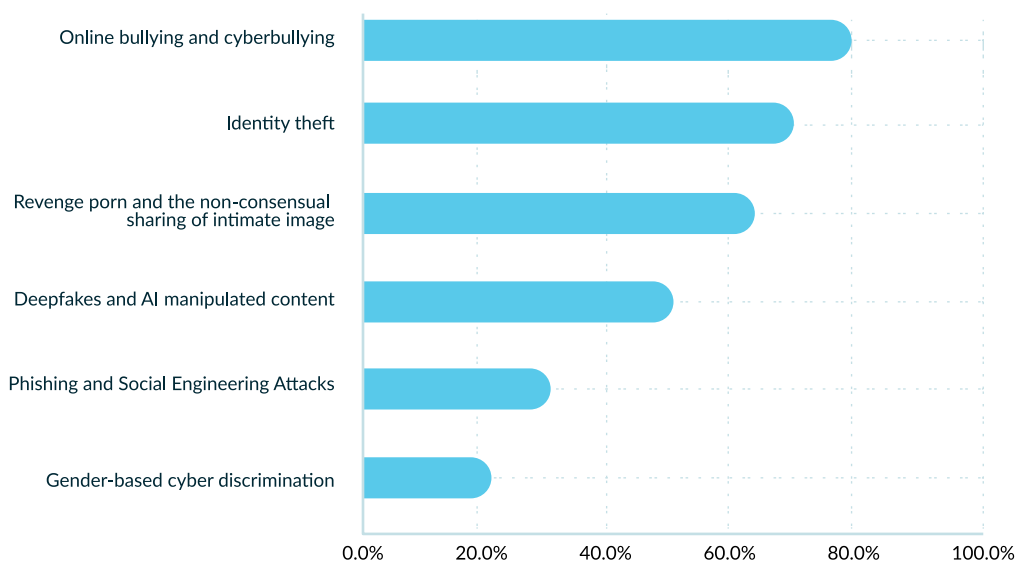


Figure 8. In your opinion, what are the most serious cybersecurity threats women face online today? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- f. Regarding the question “Do you believe there is a need for gender-specific training in cybersecurity or AI?” 57.4% of participants fully agreed, indicating strong support for tailored training programs. This highlights the belief that gender-specific approaches are important in addressing unique challenges women face in these fields and suggests a need for more inclusive educational initiatives.

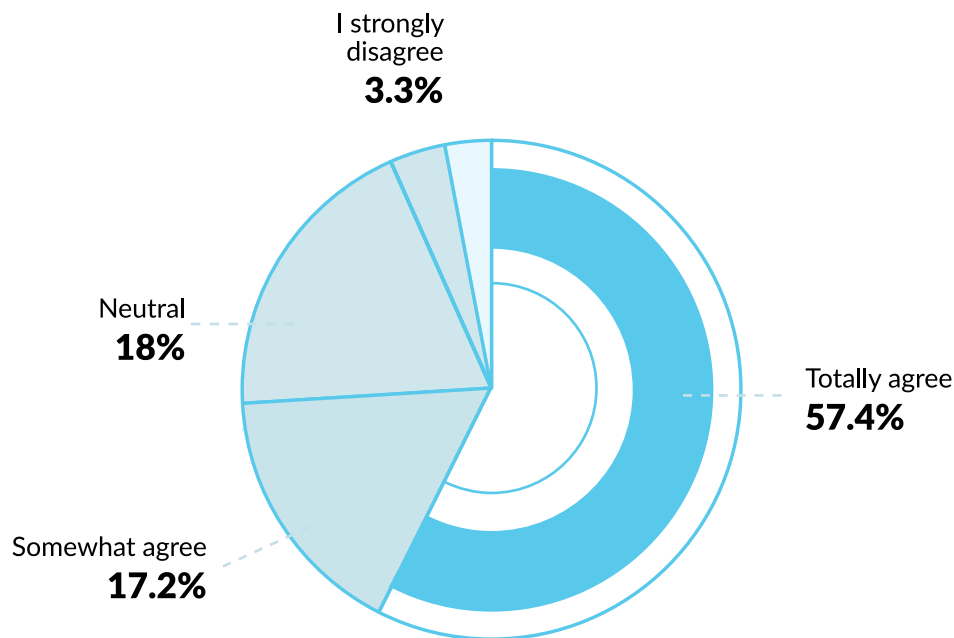


Figure 9. Do you believe there is a need for gender-specific training in cybersecurity or AI? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- g. In response to the question “How much do you know about laws in Kosovo regarding cybersecurity and data protection?” 42.6% of participants said they have little knowledge, while only 5% felt they were very well-informed. This indicates a significant gap in awareness of legal protections and cybersecurity laws, emphasizing the need for greater education and outreach in this area.

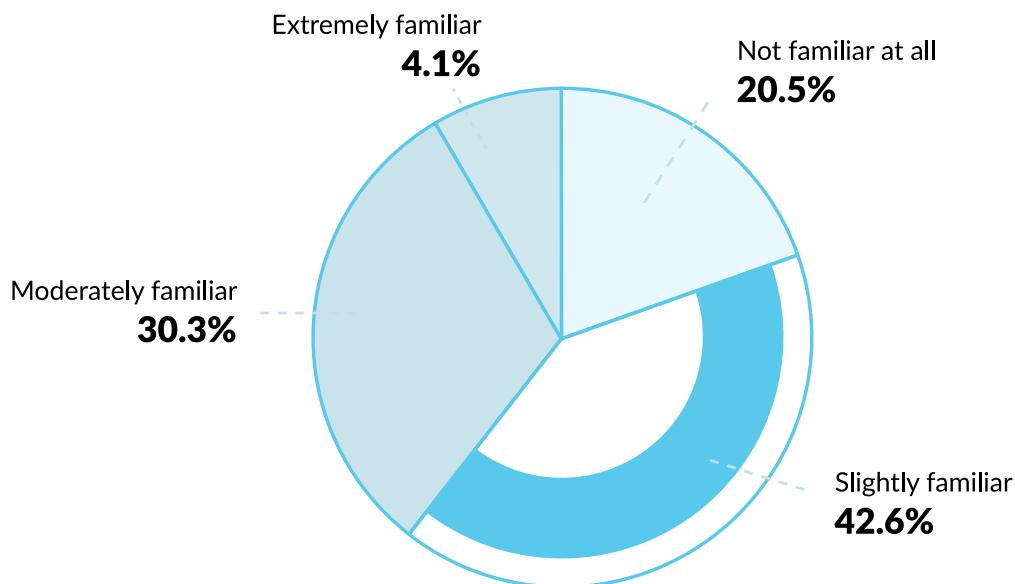


Figure 10. How much do you know about laws in Kosovo regarding cybersecurity and data protection? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- h. Addressing the question “If you were to face a cyber-threat, would you know where to report it?” 57.4% of participants responded “No”, indicating a lack of awareness about where to seek help. Among those who answered “Yes,” the most commonly mentioned institutions were the Kosovo Police, the Center for Legal Assistance, and the Ministry of Internal Affairs. These findings highlight the need for clearer guidance and public awareness on reporting cyber threats in Kosovo.

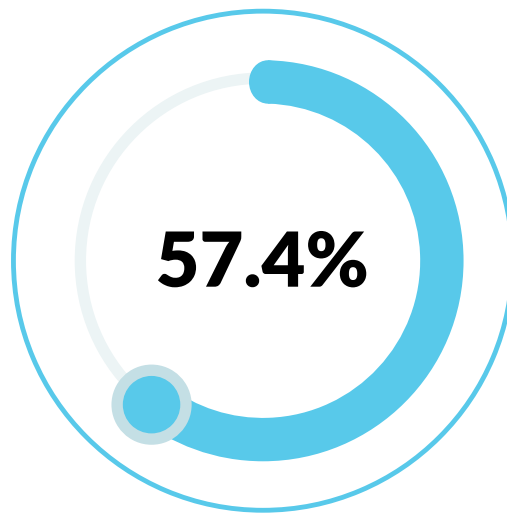


Figure 11. If you were to face a cyber-threat, would you know where to report it? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

- i. In response to the question “What actions do you think policymakers should prioritize to improve cybersecurity for women?” 50.8% of participants voted for introducing specific cyber laws for women, while 46.7% supported creating public awareness campaigns.

Additionally, 43.4% selected all of the following options:

- Introducing specific cyber laws for women
- Increasing funding for cybersecurity programs
- Creating public awareness campaigns
- Support for women in technology initiatives
- Strengthening reporting mechanisms
- Cooperation with the private sector and NGOs

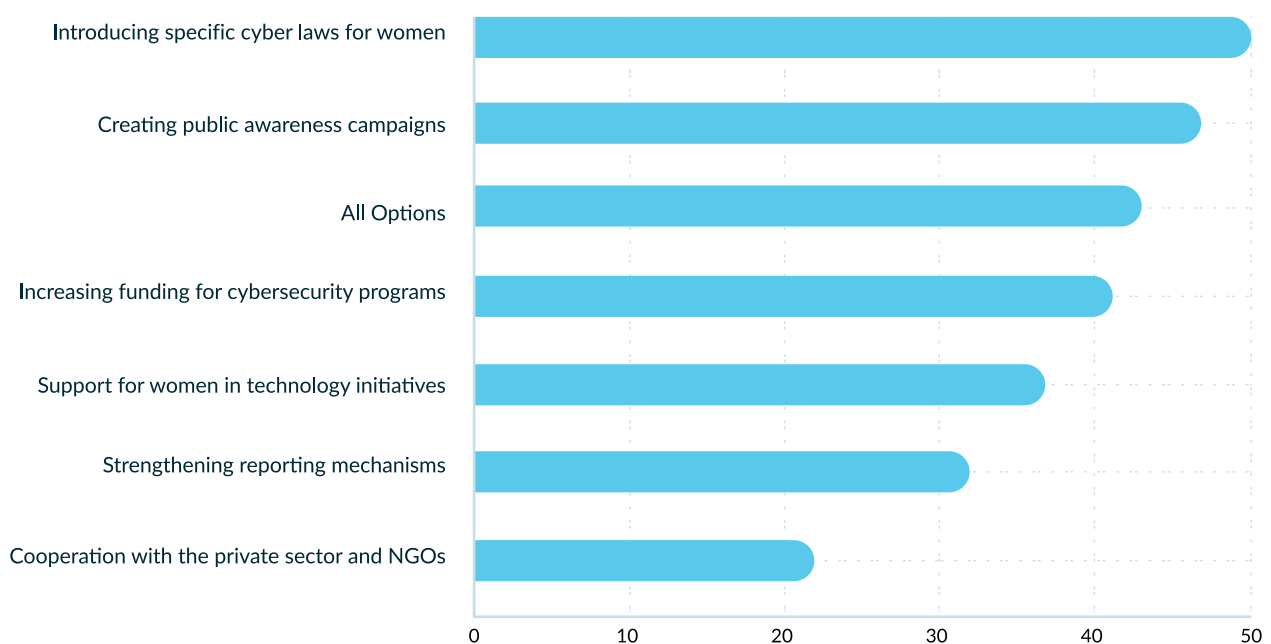


Figure 12. What actions do you think policymakers should prioritize to improve cybersecurity for women? Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

These results highlight the broad support for comprehensive strategies that include legal protections, awareness efforts, and cross-sector collaboration to enhance women's cybersecurity.

- j. In regard of the question "In your opinion, how important is advocating for women's cybersecurity to policymakers?", 73.8% of participants responded "Very important", emphasizing the strong belief that policymakers should prioritize cybersecurity protections specifically tailored for women.

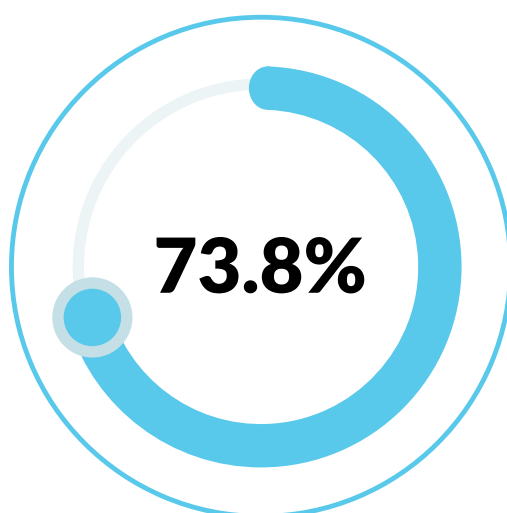


Figure 13. In your opinion, how important is advocating for women's cybersecurity to policymakers?" Data Source: Assessment Survey Summary: Kosovo Women and Their Engagement with AI and Cybersecurity, IPKO Foundation and Women in Tech Kosovo

6. Recommendations for Ethical and Responsible AI and Cybersecurity Development in Kosovo

As Kosovo continues to explore the development of its AI and cybersecurity sectors, it is essential to move beyond discussions and adopt concrete ethical principles and best practices. While progress has been made in outlining recommendations, no significant actions have been taken yet to ensure that these technologies are implemented in a way that benefits society and minimizes potential risks. The following recommendations are proposed to guide the responsible development and deployment of AI in Kosovo

- **Increase Awareness and Accessibility of Reporting Mechanisms:** Launch public awareness campaigns to educate women on how and where to report cyber threats. Collaborate with institutions like the Kosovo Police, the Ministry of Internal Affairs, and NGOs to ensure reporting mechanisms are accessible, understandable, and trusted. This aligns with transparency, ensuring that processes are clear and comprehensible to users.
- **Strengthen Legal Frameworks and Introduce Gender-Specific Cyber Laws:** Develop and implement cyber laws that specifically address gender-based cyber threats, such as online harassment and identity theft. Raise public awareness about these laws to ensure women know their legal protections. Clear accountability mechanisms must also be established, ensuring that those responsible for developing and operating AI systems are held accountable for ethical breaches or harm.

- **Expand Cybersecurity and AI Training Programs for Women:** Provide accessible, affordable, and localized training opportunities in cybersecurity and AI, focusing on underserved women. This should include ethics in design training, where women learn not just technical skills, but also the ethical implications of AI. Incorporate hands-on workshops and mentorship programs to enhance both skills and awareness of ethical standards, such as privacy and security.
- **Promote Gender-Specific Training in AI and Cybersecurity:** Design training programs tailored to address the unique challenges women face online, including cyber harassment and privacy violations. Emphasize non-discrimination by ensuring the training actively promotes inclusivity and combats bias in AI systems, helping to create a safer and more equitable online environment for women.
- **Create Public Awareness Campaigns Around Women's Cybersecurity:** Launch public campaigns to raise awareness about common cybersecurity threats to women, such as online bullying, identity theft, and non-consensual image sharing. Educate women on digital safety practices, including how AI systems impact their privacy and security. This is crucial for building trust in AI technologies, as users need to understand and feel safe engaging with digital tools.
- **Support Women in Technology Initiatives and Increase Funding:** Increase financial support for initiatives aimed at advancing women in technology, particularly in AI and cybersecurity. This includes partnering with the private sector, NGOs, and tech organizations to provide funding for scholarships and innovation hubs. Access to human rights must be a key component, ensuring that women's rights are protected and promoted through these initiatives.
- **Encourage Cross-Sector Collaboration to Strengthen Cybersecurity for Women:** Foster partnerships between government, tech companies, educational institutions, and civil society to create a unified approach to enhancing cybersecurity for women. These collaborations should also focus on building accountability frameworks, ensuring that all stakeholders involved in AI development and cybersecurity initiatives are responsible for the outcomes and impacts of their work.
- **Empower Women Through AI Tools and Digital Skills Development:** Continue offering workshops that help women improve their proficiency with AI tools and digital skills. Ensure that AI systems are developed with transparency, so that women using these technologies understand how decisions are made and have control over their usage. Provide advanced training opportunities that promote leadership and specialization in AI and cybersecurity.
- **Implement Robust Data Privacy and Security Measures:** Ensure that personal data used within AI systems is securely protected through encryption and anonymization and that AI systems comply with data protection laws. This aligns with privacy and security, essential to safeguarding individual rights and maintaining trust in AI technologies. Training programs should also emphasize these principles, teaching women how to protect their own data and understand the privacy implications of AI.
- **Increase Ethical Awareness in AI Development:** Ensure that all AI systems used or developed are aligned with ethics in design principles, including fairness, transparency, and non-discrimination. Ethical considerations should be integrated from the earliest stages of AI development to avoid harmful biases and ensure the technology is used to benefit society, including marginalized groups such as women.

7. Conclusion

7.1 The Future of AI and Cybersecurity in Kosovo: The potential impact of empowering women in these fields.

The future of AI and cybersecurity in Kosovo holds great promise, particularly as the country continues to make significant strides in both fields. One of the most transformative aspects of this progress lies in empowering women to actively participate and lead in these sectors. By equipping women with digital skills and encouraging their involvement in AI and cybersecurity initiatives, Kosovo can not only address the gender gap but also foster a more diverse and innovative workforce.

Empowering women in AI and cybersecurity offers a unique opportunity to reshape how technology is developed and implemented, ensuring that it reflects the needs and perspectives of all members of society. Women's involvement can lead to more inclusive AI applications and stronger cybersecurity protocols, which are crucial as digital threats become more sophisticated. Furthermore, initiatives such as gender-based cybersecurity training, supported by both local organizations and international partners, have shown the potential to enhance the protection of women online and contribute to a safer digital environment.

In the coming years, Kosovo's focus on advancing its National Cybersecurity Strategy 2023-2027, along with continued support for AI-driven innovation, will create new pathways for women in technology. By fostering a culture of inclusion and leveraging the talents of women, Kosovo can not only strengthen its digital infrastructure but also lead the way in developing ethical and responsible AI systems that benefit society as a whole. The empowerment of women in these critical fields is not just a step toward gender equality—it is a strategic investment in the country's digital future.

8. References

1. McKinsey Global Survey. McKinsey & Company, <https://www.mckinsey.com/capabilities/mckinseydigital/our-insights/the-top-trends-in-tech#new-and-notable>.
2. Global Index for Responsible AI. Open Data Kosovo, <https://opendatakosovo.org/wp-content/uploads/2024/06/GI-1st-Edition-Report.pdf>.
3. Law No. 06/L-082 on Protection of Personal Data. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=18616&langid=2>.
4. Law No. 04/L-094 on the Information Society Services. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=2811&langid=2>.
5. Law No. 08/L-022 on Electronic Identification and Trust Services in Electronic Transactions. Official Gazette of the Republic of Kosovo, <https://gzk.rks-gov.net/ActDetail.aspx?ActID=51618&langid=2>.
6. Kosovo Digital Agenda 2030. Government of Kosovo, <https://konsultimet.rks-gov.net/viewConsult.php?ConsultationID=41846>.
7. e-Government Strategy Kosovo 2023-2027. Ministry of Internal Affairs of Kosovo, <https://mpb.rks-gov.net/Uploads/Documents/Pdf/EN/2700/e-Government%20Strategy%20Kosovo%202023-2027.pdf>.
8. Hamzaj, Genc. Interview. Conducted by Blerta Thaçi and Dafina Olluri, 25 Sept. 2024. Information Society Agency, <https://ashi-upi.rks-gov.net/en>.
9. Kosovo Law Ignores Tech-Facilitated Abuse of Women, BIRN Report. Balkan Insight, 25 June 2024, <https://balkaninsight.com/2024/06/25/kosovo-law-ignores-tech-facilitated-abuse-of-women-birn-report/>.
10. "Code of Lekë Dukagjini." Wikipedia, https://en.wikipedia.org/wiki/Code_of_Lek%C3%AB_Dukagjini.
11. "TikTok Used Across Balkans to Slutshame Women and Girls." Balkan Insight, 6 Mar. 2024, <https://balkaninsight.com/2024/03/06/tiktok-used-across-balkans-to-slutshame-women-and-girls/#:~:text=A%20BIRN%20analysis%20of%20hundreds,sexual%20behaviour%20%2D%20'slutshaming>.
12. Kosovo Assembly Official Website. <http://old.kuvendikosoves.org/?cid=2,191,103>.
13. Limani, Myzafere. Akademia e Shkencave dhe e Arteve e Kosovës, <https://ashak.org/anetaret/myzafere-limani/#:~:text=Biografia.%20Myzafere%20Krasniqi-Limani%20e%20lindur%20n%C3%AB%20Pej%C3%AB%20m%C3%AB>.
14. Komoni, Vjollca. Professor of Electrical Engineering, University of Prishtina. Google Scholar, https://scholar.google.com/citations?user=7hz_5LoAAAAJ#:~:text=Articles%201%E2%80%9318.%20%E2%80%AAProfessor%20of%20Electrical%20Engineering,%20University%20of.
15. Sahatqija, Teuta. "Success Story: Women in Tech." TACSO, <https://tacso.eu/story/success-story-women-in-tech/>.
16. Alija Shala, Gentiana. "A Sustainable Future Comes from Women Changemakers." UNDP Eurasia, <https://www.undp.org/eurasia/stories/sustainable-future-comes-women-changemakers#:~:text=Gentiana%20Alija%20Shala%20is%20a%20solar%20energy%20engineer>.
17. Implications of AI Adoption on Kosovo's Tech SMEs. Rochester Institute of Technology, <https://repository.rit.edu/cgi/viewcontent.cgi?article=12972&context=theses>.
18. "AKSK Organizes 'Cyber Fortress 2024': A Digital Battle for Cybersecurity Experts from Albania and Kosovo." Albania Tech, 25 July 2024, <https://albaniatech.org/aksk-organizes-cyber-fortress-2024-a-digital-battle-for>

19. "Conference on Privacy and Security." Facebook, <https://www.facebook.com/share/p/eGy7n9BgWHRGAVvy/>.
20. "Cyber Defense Competition." LinkedIn, https://www.linkedin.com/posts/blera_iowa-kosova-fsk-activity-6932957138457657344-pPVD/.
21. "Girls in Cyber." Facebook, <https://www.facebook.com/share/p/nqhaFhddpTjEuXuP/>.
22. Kosovo Cyber Team. <https://kosovacyber.team/>.
23. European Cybersecurity Challenge 2024. LinkedIn, <https://www.linkedin.com/company/ecsc2024/>.
24. European Union Agency for Cybersecurity (ENISA) - European Cybersecurity Challenge 2024. <https://ecsc2024.it/>.
25. BSides Prishtina. <https://bsidesprishtina.org/>.
26. Berisha, Albulena Xhelili, and Inta Plostins. "How Multi-Stakeholder Coalitions Can Enhance Policy and Regulatory Frameworks for Cybersecurity." DAI Global Digital, 25 Apr. 2024, <https://dai-global-digital.com/how-multi-stakeholder-coalitions-can-enhance-policy-and-regulatory-frameworks-for-cybersecurity.html>.
27. "Cyber Unity: Cyber Security Training." Innovation Centre Kosovo, <https://ickosovo.com/training/courses/cyber-unity-cyber-security-training1>.
28. "RIT K Students in International Cybersecurity Exercise 2024." RIT Kosovo, 26 Feb. 2024, <https://www.rit.edu/kosovo/news/rit-k-students-international-cybersecurity-exercise-2024>.
29. "Global Index on Responsible AI." Open Data Kosovo, <https://opendatakosovo.org/portfolio/global-index-on-responsible-ai/>.

ipkofoundation

**WOMEN
in·tech[®]
KOSOVO**

NL Netherlands