Security Implications of Social Robots in Public Space – A Systematic Literature Review

Fabien Sechi

Department of Risk, Safety, and Security, Institute for Energy Technology, Norway. E-mail: fabien.sechi@ife.no

Yonas Zewdu Ayele

Department of Risk, Safety, and Security, Institute for Energy Technology, Norway. E-mail: yonas.ayele@ife.no

Social robots are increasingly becoming ubiquitous from healthcare to our homes. When it comes to the state-of-the-art autonomous social robots and artificial intelligence (AI) are typically designed in a way that they adapt and optimise their behaviour over time as more knowledge of their environment is gained. This entails some sort of data gathering, storage, and processing that is used as a basis to improve the robot’s behaviour. If we assume that the AI of social robots soon will evolve, adapt, and learn from its context and optimize the user experience, a question is how to assure end-users security. A challenge is that the capabilities of modern AI and social robots for public space evolve rapidly, and there is a lack of knowledge on how to assure by design a continued level of security for end-users that interact with such systems. Further, in most of the available social robot and cyber security literature, the security implication of social robots in public space has received less attention. The overarching purpose of this paper is thus to understand and scrutinize the security principles and guidelines for social robots operating in public spaces. In connection to this, the paper addressed the following two research questions:

i) what are the security, safety, and privacy principles and guidelines suitable for application to social robots in public spaces; and

ii) what legal differences in are principles and guidelines between robots in public and private spaces. The results depict that though there are several potential cyber technical and information security risks associated with social robots, there are also various security features, which can be used to mitigate these risks.

Keywords: social robots, human-robot interaction, security, public space, cybersecurity, privacy, safety

1. Background

As social robots are increasingly becoming ubiquitous, one must understand the security implications of social robots before the introducing of new social robots into our public space (Given-Wilson, Legay, and Sedwards 2017). This is to protect against security, safety, and privacy-related issues from all potential threat sources. A security risk assessment would be performed along with the safety assessment of the social robot. Periodic security risk assessment and audits would be conducted to update the security risks associated with the social robot to have an up-to-date security posture and increase the visibility aspect. However, a challenge is that the capabilities of modern social robots for public space evolve rapidly, and there is a lack of knowledge on how to assure by design a continued level of security for end-users that interact with such systems, see e.g. (Salvini, Paez-Granados, and Billard 2021), (Andriella, Torras, and Alenyà 2020), and (Cubric 2020).

In connection to this, this paper employed a systematic literature review (SLR) to address two research questions: i) what are the security, safety, and privacy principles and guidelines suitable for application to social robots in public spaces; and ii) what legal differences in are principles and guidelines between robots in public and private spaces. Addressing these questions would improve the understanding of security, safety, and privacy principles and standards and assess the preparedness of the social robot operators to handle incidents. This, for example, will ensure that cybersecurity incident response plans and procedures are in alignment with safety planning.

The SLR has focused on knowledge-gathering, to:

• Identify and analyse the current state-of-art or knowledge related to the security of social robots;
• Recognise the indicators used by social robot organisations to secure their robot;
Identify articles, reports, and information on the application of security for social robots;
Assess the current state of practice via interviews with robot manufacturers, security experts, and citizens.

The rest of the paper is organised as follows: Section 2 depicts a bird’s eye view of social robots’ aspects. Section 3 presents the research questions and, the SLR approach. Section 4 provides a discussion of the results from the SLR. Concluding remarks are depicted in Section 5.

For this paper, social robots as “a physical entity embodied in a complex, dynamic, and social environment sufficiently empowered to behave in a manner conducive to its own goals and those of its community” (Duffy et al. 1999).

2. Social robot’s aspects: A bird’s eye view

In general, social robots are robots with social interaction capability; and, when working in a public space they encounter a bigger threat landscape and might meet an even bigger diversity of individuals (Whittaker 2022). Henceforth, social robots should be safe, and secure, and follow and respect the legislation, such as user data privacy, based on the existing principles and guidelines. Safety standards must evolve.

Safety aspects: To comply with the safety requirements and legislation, robot designers must consider autonomy's physical, social, and ethical effects. Further, to assuring people's safety, robots must work towards maintaining or improving human abilities in addition to their capabilities (Murashov, Hearl, and Howard 2016). For instance, (Salge 2017) demonstrated that the design of the robot must ensure that the robot's actions are predictable to humans and will not produce unpleasant reactions such as fear, shock, or surprise.

Security aspects: For a robot to be safe, it must be also secure Tanya M. Anandan (2018). When it comes to the security aspects of social robots, one must be more vigilant beyond the technical aspects. In this connection, there have been several studies. For instance, the Kaspersky Lab and the University of Ghent research team examined how the widespread use of so-called "social robots" in the future could affect people's security, privacy, social behaviour, and who they are, see e.g. (Galov 2019).

The need for security guidelines: Robust security policies are professionally designed to enhance security and demonstrate a sustained commitment to achieving the required robotics and cybersecurity requirement. For instance, Safety Requirements Analysis analyses safety requirements to formulate effective control policies and procedures that will be applied in the field of robotics (Yaacoub et al. 2022). In addition, see e.g. Tanya M. Anandan (2018), TUV Rheinland’s Stanley recommends that robot manufacturers should ensure that their products meet as many of these requirements as possible.

User data privacy aspects: The strict new EU General Data Protection Regulation (GDPR) have affected companies around the world, including social robot developers and operators. Back in 2012, the European Commission proposed reforming GDPR rules to strengthen online privacy, see e.g., (van der Shaft 2018). Thus, to fully utilise GDPR, end-users of social robots should be aware of its provisions.

Legal aspects: As (Joh 2016) depicts life is opposed to property; however, robots can belong to a legal category that is neither purely property nor people. This dilemma might lead to a legal issue. For instance, if a robotic company does not have a human owner, there is no "simple" theory of subsidiary liability for the courts to judge its actions (Espelien 2016).

3. Methods

As described above, to answer the questions better, (Kitchenham 2004) systematic review guidelines have been employed to synthesize the extant literature about the safety, security, and legal aspects of social robots. The starting point of the SLR is verifying that there are no other SLRs published in similar scopes. In connection to this, the verification process provides an SLR by (Góngora Alonso et al. 2019) that describes the social robots and security aspects, for People with Aging and Dementia. However, this SLR hasn’t explicitly explored the diverse security implications that could be applied.
To reiterate, the research questions (RQ) for this SLR are: i) what are the security, safety, and privacy principles and guidelines suitable for application to social robots in public spaces; and ii) what legal differences in are principles and guidelines between robots in public and private spaces. Further, to supplement these research questions, we have formulated three predominant refined research questions (RRQ) as follows:

- RRQ1: What are security principles and guidelines that can be applied to social robots?
- RRQ2: What are safety and privacy principles, and guidelines that can be applied to social robots?
- RRQ3: What are the legal principles and guidelines, regarding security and safety, that are unique to public space robots rather than private space robots?

3.1. Eligibility criteria

The study is eligible for SLR based on the following Inclusion Criteria (IC), Exclusion Criteria (EC), and Quality Criteria (QC). The IC helps to refine the result for EC; and, if the study fulfills at least one EC, it would be removed from the SLR. In addition, when it comes to QC, a study is removed, if the overall score of QC is less than 70 per cent (see Section 3.3).

The IC used are: IC1: That the word social robot or security in at least one example from the title or topics, the search string gives us 225 results, IC2: The work has been published in the last 7 years; years from 2016, the search string gives us 177 results with a period from 2016 to 2021 and, IC3: That the work has been published in the English language.

The IC used are: IC1: That the word social robot or security in at least one example from the title or topics, the search string gives us 225 results, IC2: The work has been published in the last 7 years; years from 2016, the search string gives us 177 results with a period from 2016 to 2021 and, IC3: That the work has been published in the English language.

We the used, the following EC: EC1: Social robot substring does not appear in the title abstract and in the keywords, EC2 The work is a duplicate of another work, only one is kept with the most citation first or the newest and EC3: 1-pager publications.

The study QC are (Table 1):

- QC1: Is the aim of the research identified clearly (Two criteria for QC1: QC1.1 robot and QC1.2 security)?
- QC2: Are the results of robots and security clear and concise?
- QC3: Are weaknesses in the work explicitly identified (validity threats)?
- QC4: Was the proposed principle or guideline developed on a detailed level following a rigorous and/or formal methodology?
- QC5: Was the proposed principle or guideline developed considering ethical aspects?
- QC6: The title contains both substrings’ keywords?

3.2. Extraction Group

To extract the information from the above 8 literature, in this study we have used seven groups. These groups (Gs) are: G1: Publication identification, G2: Social robots, G3: Security, G4: Safety and privacy principles, G5: Legal with moral and ethics.

3.3. Data collection process

Fig. 1 depicts the data collection process for our SLR. The automatic search was performed through the Web of Science (WoS) (‘Clarivate’ 2022). WoS comprises renowned publishers of different kinds of conferences and journals such as ACM Digital Library, Elsevier, Wiley, Springer, Sage, Taylor & Francis, and MIT Press.

Fig. 1 Search process and structure

By using the term social robots and security mechanisms, 566 studies have been extracted from WoS. A further 398 pieces of literature have been excluded based on the three IC defined above. In addition, 135 studies have been eliminated because of the ECS stetted for our SLR. Consequently, only 8 studies were finally included in this SLR (see Table 1).
Table 1. Extract of QC highest score, out of 33

<table>
<thead>
<tr>
<th>Paper ID</th>
<th>QC</th>
</tr>
</thead>
<tbody>
<tr>
<td>P1</td>
<td>1.1 1.1 1.1 1.1 1.1 1.1 7</td>
</tr>
<tr>
<td>P2</td>
<td>1.1 1.1 1.1 1.1 1.0 1.0 6</td>
</tr>
<tr>
<td>P3</td>
<td>1.1 1.1 1.0 1.1 1.0 1.0 6</td>
</tr>
<tr>
<td>P4</td>
<td>1.1 1.0 1.1 1.0 1.0 5</td>
</tr>
<tr>
<td>P5</td>
<td>1.1 1.1 1.1 1.0 0.0 5</td>
</tr>
<tr>
<td>P6</td>
<td>1.1 1.1 1.1 1.0 0.0 5</td>
</tr>
<tr>
<td>P7</td>
<td>1.1 1.0 1.1 1.0 5</td>
</tr>
<tr>
<td>P8</td>
<td>1.1 1.1 1.1 1.1 1.1 7</td>
</tr>
</tbody>
</table>

Based on the QC, the overall score of more than 70 per cent, 8 papers (Ps) from P1 to P8.

3.4. Data search string

The search string used in this SLR has three parts:
- Part I of the search string is aiming to extract papers related to the social robot as defined for the social robot substring. The difference between Part I and the search result for “social robot*” is 251 results “ALL=(social robot*) NOT #1”.
- Part II of the search string is aiming in investigating different security technics and guidelines as defined for the security substring. The difference between Part II and the search for “*security” is of 22899 results “(ALL=(security) OR TS=(security)) NOT #2”.
- Part III of the search string aims in extracting the most relevant results based on Part I and Part II as defined for the search string. The difference between Part III and the search result for “social robot**” and “*security” is 14 results.

4. Results and discussion

In this section, the results have been categorised based on the extraction groups (Gs).

*Based on G1:* Computer science is the most popular research domain among the papers in the set, followed by robotics, cybernetics, and theory/methods. Interdisciplinary applications, including AI, are also represented but to a lesser extent. Papers titles are mostly focused on the topics of security, privacy, and legal perspectives surrounding social robots. Other topics include usability perceptions and gender recognition systems. Papers published in 2021 are the most frequent, while papers published in 2017 and 2019 are the least frequent. The first author has a significant influence on the set of papers. Most professions are mainly academics title and sometimes they also have an Engineering background, such as cybersecurity or software. Only P1 has non-academic affiliations within the author list. The most relevant keywords are security, domestic robot, and social robot.

Most of the selected papers are journal papers 62.5% against conference papers 37.5%. CHI 2018 conference can be considered a good Impact Score (IS>3) and Science robotic journal can be considered of excellent quality (IS>9). However, IS is not the only metric that should be considered to evaluate the quality.

For instance, P1 is discussing the rise of robots in the industry and their impact on security and privacy. P2 illustrates the challenges of designing robots that are inclusive of transgender individuals. While P3 depicts the Acanto project and the challenges of developing a robotic assistant that is secure and private. P4 highlights the ten challenges of robotics research. P5 presents details about robot-assisted training and its impact on safety and security. P6 depicts the use of data mining in the design of robotic products. P7 elucidates the development of a security-enhanced Robot Operating System (ROS). P8 clarifies the impact of perceived security, privacy, and legal concerns on the attitude and intention toward robots. Based on the G1, it can be deduced that end-users in general have negative attitudes towards Automatic Gender Recognition (AGR) because it can accurately recognize such a subjective aspect of their identity. In addition, when social robots are being used as motivational coaches, the pieces of the literature suggest that feedback given by a robot agent can influence the various facets of participant experience in robot-assisted training.
Further, data from two crowdfunding sites (Kickstarter and Indiegogo) suggest that health and fitness, security and monitoring, general education applications, cartoon-like, and animal-like robot forms, and single-user group robots have significantly more backers.

Moreover, there is also a clear sign of growing the interest of hackers parallel to the increasing adoption of humanoid social robots in different application fields. This would violate people's privacy or even worse-threaten humans' lives from physical and emotional/social points of view. Likewise, as domestic robots, also known as companion robots or social robots, usage increases, people are starting to perceive different kinds of security, privacy, and legal usage issues.

**Based on G2:** Nowadays, there exists a robot technology with social features such as a) Robot assistants as smart speakers, b) programmable artificially intelligent humanoids, integration, and fundamental aspects, c) biometric features as implemented with AGR, d) walker robot for autonomy paired with the social network, and e) domestic robot.

The results based on G2 illustrate that there are non-commercial research social robots such as P3 Friwalk; and “commercial off the shelf” as Google Home®, Amazon Echo®, Softbank robotic NAO®, and Pepper®, EZ Robot JD®. In addition to this, there are also crowdfunded robot as JoyForAll Cat®.

It can be also deduced that there are different contexts in forming robot use. In some cases, the robot is used for demonstration purposes, while in others it is used for actual tasks such as mobility assistance or security. Likewise, there are also robots used as a model for understanding social interaction.

When it comes to pricing, our results show that there is no standard price for a social robot. The price varies depending on the features and functionality. And, the results also depict that when it comes to knowledge areas, the most useful areas for building a social robot are social interaction, security, privacy, ethical issues, usability, trust, cyber-physical systems, and Human-Robot Interaction (HRI).

Regarding social robot definitions, the 8 papers assessed in this SLR, have different views on the definition.

The main difference is that P1, P2, P3, P6, and P8 mainly emphasised interaction with humans while P4, P5, and P7 mainly focused on the design and function of social robots. Further, P1, P2, P4, P5, P6, and P8 provide a more detailed and comprehensive definition of social robots compared to P3 and P7. P7 is the only paper that mentioned the potential risks of social robots. P1 has focused on the social robot as “a physical entity embodied in a complex, dynamic, and social environment” which is different from P2 to P8, where they focused on the social robot lasthe one that “interacts with humans” but they add on different aspects such as “provides unique solutions to usable security and privacy problems”. And, P2 highlights social robots “collect and analyze sensitive data from users” and can pose a security and privacy risk if users are not properly informed about how to protect their information.”

**Based on G3:** In general, G3 is highly correlated with RRQ1. Here, we found out that when it comes to the definition of “security”, P2, P3, P4, and P5 emphasised mainly users and people, and the human side of it, primarily the sense of security. It could be seen as more like a feeling. In other words, as a field of study, that deals with protecting people, property, and information from harm or loss. Or the need to protect user information from being accessed or used without permission. Or something that helps to ensure that interacting with robots is a safe and positive experience for users. Or a state of being protected from physical and psychological harm during the interaction with a robot.

In addition, regard “robot safety”, which generally is the study of how to protect users, property, and information from harm or loss when interacting with robots. In connection to this, P1, P6, P7, and P8, focused on the device’s technical side, the surveillance, and the monitoring aspects. It could be seen as more like a function. That means the degree to which a device or system can protect users’ data and information from being accessed or compromised by unauthorized individuals or entities. Or a function that can be added to robots in other application areas. Or something that has been recently added to ROS in the form of security enhancements. And an effective legal framework to address privacy and security concerns of domestic robots.
Further, the results show that P1 and P2 were mainly surveyed to get people's security opinions. Yet, P3, P4, and P7 proposed security methods and advanced technical security upgrades, while P5 and P8 collected opinions about the sense of security and security perceived based on a questionnaire-based survey. Yet, P6 squared security information characteristics of the robotic product. Our results depicted that the use of space and area settings for security methods and robots is mostly for private space settings. However, some of the literature illustrates the security aspects could also be used for public spaces, such as in a hospital setting in public space where physical attacks are of higher concern.

When it comes to security domains, the results show that the main domains are security, social, ethical, psychological, marketing, cybersecurity, and technical. Further, regarding guidelines used in the 8 literature that we have studied, P2 employed a NIST for the internal report on the face recognition vendor test to classify algorithms' performance. P6 and P7 used a guide to understanding different types of robots and all methods cited have a reference with guidelines in standards for secure data in transit as TLS, PKI, and AES. They have also referenced principles as an evaluation methodology for security bystander role of interaction and vulnerability principle common vulnerability enumeration (CVE) are not specific for the robot.

Overall, our results illustrate that there are many potential security risks associated with social robots, but there are also some potential security features that can be used to mitigate these risks. Further, the phase and time where security principles and guidelines can be applied in the lifecycle of the robot vary depending on the type of security technique being used and the specific application or context in which it is being deployed. However, in general, most security principles and guidelines can be applied during the design and development phase of a robot's lifecycle, as well as during its operation and maintenance. For instance, P1, P5, and P8 showed how can understanding security and usage can help increase security or change usage.

Likewise, P2, P4, and P6 demonstrated how understanding; technology ethics can help future security development, the operation and usage of current technology can help social robot security developers develop them more ethically and securely, and the market share of robots can help build more attractive robots in terms of features.

*Based on G4:* G4 directly correlates with RRQ2.

Privacy and security concerns are key factors in people's perceptions of humanoid social robots, and these concerns must be addressed for the technology to be widely adopted. Differential privacy is one potential solution to the issue of handling sensitive data, and manufacturers need to build controls into their robots to reduce the scope for privacy infringement.

Furthermore, appropriate legal frameworks need to be implemented for social robots to protect against privacy and security vulnerabilities. It is important to consider issues of security and privacy regarding the use of domestic robots and expected that households will use a domestic robot when they perceive that its usefulness will exceed the security and privacy risks and concerns.

From our results, it can be deduced that all references cited in P1, P2, P5, P7, and P8 supported the claim that "privacy is needed in technology". Yet, P1 is the only paper without a discussion about safety concerns. P2 to P8 illustrated the concept of safety as the state of being free from harm or danger. The concern about AGR reinforcing gender binaries and how that could override user autonomy was also discussed in these two papers. Likewise, the user's perceived state of being protected from physical and psychological harm during the interaction with a robot is important in HRI. There are also legal frameworks in place to protect people's data and privacy when using domestic robots.

*Based on G5:* This is associated with RRQ3.

In this regard, our results demonstrate that P2, P3, P4, P6, and P8, depict legal as an area where there is a need for improvement in the way that AGR technology is used. Or a requirement that must be met to prevent issues, a challenge that can be easily resolved by complying with all legal requirements in different countries.
Or a set of rules and regulations designed to protect people's rights and safety, and an aspect of domestic robot usage that must be considered to ensure that these devices are used safely, securely, and without violating anyone's privacy.

Further, P1, P2, P4, and P8 illustrate about ethics as something that must be taken into consideration when developing new technologies that have the potential to impact people's lives. Also, the concept of morals, based on P2 and P4 is something proper to the individual making technology. P4 defined morality as the ability to reason about right and wrong; act in accordance with social and moral norms; learn the appropriate social and moral norms for a particular setting, and finally adapt to cultural differences.

Overall, our results demonstrated that there was no precision in the use of an ethical, moral, or legal framework related to social robots operating in public spaces. This can be explained by the fact that they need to be linked to a physical or moral person, environment, and different law regulations.

5. Conclusion

This work carried out a systematic literature review (SLR) to understand the security, safety, privacy as well as legal aspects related to social robots operating in public spaces. The results depicted that there are many potential cyber technical and information security risks associated with social robots, but there are also some potential security features that can be used to mitigate these risks. When it comes to safety – it is important to consider issues of security and privacy associated with the use of social robots. The results also proved that it is expected that households will use more and more social robots when they perceive that their usefulness will exceed the security and privacy risks and concerns.

Regarding privacy – social robot manufacturers need to build controls into their robots to reduce the scope for privacy infringement. They should also communicate better with the public or authorities, e.g., by being more transparent about the security features of their robots.

Furthermore, our results pointed out that appropriate legal frameworks should be implemented for social robots to protect against privacy and security vulnerabilities.

When it comes to legal – there is a need for improvement in the way that biometrics technology and user information are used, and a set of rules and regulations designed to protect all people's rights including minorities and safety must be complied with to prevent issues especially when the boundary from private to public space open.

Acknowledgement

The work has been partially funded by The Research Council of Norway through the SecuRoPS “User-Centred Security Framework for Social Robots in Public Space” project facilitated at Institute for Energy Technology, Halden, Norway. The financial support was gratefully acknowledged.

References


2315
Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)


