PRIVACY AND DATA PROTECTION CHALLENGES IN SEARCH AND RESCUE ROBOTICS: A CYBER LAW PERSPECTIVE

V. Mathivadhani Kandiyar, B.A. LL.B. (Hons), Sastra Deemed University

ABSTRACT

The increasing use of Artificial Intelligence (AI enabled search and rescue (SAR) robots has transformed disaster response by improving operational efficiency and reducing risks to human rescuers. These Artificial Intelligence are equipped with technologies such as cameras, thermal sensors, GPS, and wireless communication systems, these robots collect and process significant amounts of personal, biometric, and location based data during rescue operations. While this data collection is very important for responding to emergencies. It raises serious concerns regarding privacy, data protection, responsibility , liability and cybersecurity, particularly where information is collected without the consent of affected individuals. This research focuses on the issues related to privacy, data protection and cybersecurity regarding AI driven search and rescue robots from the perspective of cyber law. In addition, the paper discusses the ability of current cyber and data protection laws to regulate the process of collecting, processing, storing, retaining, and disclosing personal data during emergencies while ensuring the fundamental right to privacy is not violated. The paper explores issues related to accountability and liability for any problem, abuse, unauthorized access, inaccurate processing, and cyber threat resulting in a breach of data from the AI driven SAR robots. The study uses a doctrinal research methodology and examines the existing legal and regulatory framework applicable to the use of AI enabled search and rescue robotics and to assess the challenges and regulatory gaps associated with the collection and processing of data during emergency situations.

INTRODUCTION

Search and rescue (SAR) technologies that engage AI are increasingly becoming a part of the disaster response operations. Such technologies include aerial drones, wheeled robots, tracked robots, legged robots, robotic cameras, thermal imagers, microphones, global positioning systems (GPS), wireless communication systems and AI analytical software. These SAR technologies help the rescue teams in accessing hazardous, difficult to reach or unstable locations that might prove to be difficult for human access either in terms of timings or danger.

Usage of these technologies is apparent in response operations carried out in India. For instance, in a cave in the SLBC tunnel located in Nagarkurnool district, Telangana, which occurred on 22nd February 2025, technological devices such as drone cameras, robotic cameras and endoscope cameras were used by rescue teams to acquire visual data from dangerous locations. This was done through the collaboration between the National Disaster Response Force (NDRF), the army, government agencies and private technology firms. There were also communication systems to facilitate transfer of live data from the robot to the control room[1].

Similarly, after the disaster occurred in Chamoli, Uttarakhand, in 2021, the drone search missions and damage assessment was done by EndureAir Systems, which was a developing company at IIT Kanpur, in collaboration with NDRF. Live high definition images were sent by the drones to those areas where rescuers could not reach due to their accessibility issues[2]. Also, during the compassionate effort made by India in response to the 2025 earthquake of Myanmar, the Indian Army used SAR Robo Mules and nano drones fitted with thermal imaging sensors for technical assessment and rescue purposes[3].

However, the employment of SAR robots raises significant legal issues. The SAR robot which employs AI is more than just performing its physical duties. The SAR robot gathers information from its cameras, thermal sensors, microphones, GPS devices, and other kinds of sensors; it transmits this information to a command center and it even uses AI for detecting persons,

[1] Ministry of Home Affairs, Gov't of India, *Brief Report Regarding Tunnel Collapse Incident in the District—Nagarkurnool, Telangana* (Mar. 13, 2025), https://ndmindia.mha.gov.in/ndmi/viewUploadedDocument?uid=NEW2428.
[2] Indian Institute of Technology Kanpur, *EndureAir Systems, a SIIC IIT Kanpur Incubated Company* (Feb. 18, 2021), https://www.iitk.ac.in/endureair-systems-siic.
[3] *Army Deploys Robotic Mules, Nano Drones in Earthquake-Hit Myanmar*, Tribune India (Apr. 11, 2025), https://www.tribuneindia.com/news/india/army-deploys-robotic-mules-nano-drones-in-earthquake-hit-myanmar/.

dangers, objects, or even routes. As a result, the aforementioned technology gathers visual, audio, thermal, biometric, and location information not only regarding the trapped person but also regarding residents, rescuers, and even private property.

Firstly, there is the issue of responsibility and liability. Many individuals and organizations could be involved in the process of running a SAR robot, such as a governmental agency, disaster management organization, NDRF team, armed force team, incident commander, human operator, robot manufacturer, software provider, AI provider, cloud service provider or communications provider. If something goes wrong, such as the malfunctioning of the robot, inability to detect a survivor, wrong result, any physical injury, gathering of unnecessary information or a cybersecurity threat, it might be hard to figure out who should be held accountable. The issue of responsibility includes the duty to control, take care of, supervise and oversee the situation.

Secondly, the problem of privacy and data protection emerges. According to the verdict in the case of Justice K.S. Puttaswamy (Retd.) v. Union of India, privacy is considered to be a fundamental right in accordance with Article 21 of the Indian Constitution[4]. The principle of information privacy constitutes an integral element of this right. Every violation of the privacy principle should meet three Principles of legality, legitimate aim and Balanced . Rescue during disaster is a legitimate public aim without any doubt, but it does not mean that no limitations exist at all.

The Digital Personal Data Protection Act, 2023 is the primary legislation governing digital personal data in India. Section 7 states that the following processing activities shall be considered a legitimate activity in respect of personal data if they are required to ensure the protection of an individual in the event of a natural disaster or breakdown of law and order[5]. This section is significant because it would be impossible to obtain consent from individuals who are trapped, injured, unconscious, or missing. It is relevant to note that the legislation does not govern AI enabled SAR robotics.

Security of information from cyber attacks is another issue which is relevant due to the fact that SAR technology relies on wireless connectivity, sensors, GPS, control room software, and

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[5] Digital Personal Data Protection Act, No. 22 of 2023, § 7(h), India Code, https://www.indiacode.nic.in/handle/123456789/22037 (India).

even the cloud. Any breach of privacy through hacking into the system for accessing cameras, interfering in video transmission, or altering location information and artificial intelligence outputs can constitute a risk not only to the privacy but also to the safety of the entire operation.The main aim of this research is therefore to examine whether India's present constitutional, data protection, cyber law and disaster management framework adequately regulates AI-enabled SAR robots. The study investigates responsibility, liability, privacy, data protection and cybersecurity in the context of emergency robotics.

LITERATURE REVIEW

The current literature on search and rescue (SAR) robotics mainly focuses on the technological aspects of such robots, which include their operations in dangerous situations, survival detection and assistance to human rescuers, there is an emerging trend of research that focuses on the ethical, privacy and data protection issues related to the application of robots and drones in emergencies and dangerous situations. However, all these issues have mostly been addressed in isolation, and very little research has been conducted that takes all of these factors into account under the Indian law. The following are some of the most relevant journal articles and studies for the current research.

In the article "Ethical Concerns in Rescue Robotics: A Scoping Review," Linda Battistuzzi, Carmine Tommaso Recchiuto and Antonio Sgorbissa explore the ethical problems resulting from using robots for search and rescue operations. The key ethical concerns highlighted by the researchers include seven areas of importance: issues of fairness and discrimination, false or unrealistic expectations, replacement of workers, privacy, responsibility, safety and trust[6]. It is especially important to note that the robots used during the operations can acquire data about both the victims, rescuers, residents and other people who are present at the place where the disaster took place.

The importance of this article in the current research is that it has established that privacy and responsibility are integral to rescue robotics and not separate legal concerns. The operation of a rescue robot can be done by different parties that include human operators, the manufacturer of the robot, software designers, and the rescue organisation. This would mean that in case there is any malfunctioning of the robot or an incorrect result, it would be difficult to establish

[6] Linda Battistuzzi, Carmine Tommaso Recchiuto & Antonio Sgorbissa, *Ethical Concerns in Rescue Robotics: A Scoping Review*, 23 Ethics & Info. Tech. 863, 863–65 (2021)

responsibility. Thus, the article gives an important ethical basis for studying accountability and liability in SAR systems equipped with AI. However, the authors do not discuss these issues from the perspective of a particular national data protection or cyber law and also not from the Indian legal position.

The technical aspect of SAR robotics from an AI perspective is discussed in "Survivor Detection Approach for Post Earthquake Search and Rescue Missions Based on Deep Learning Inspired Algorithms" by Rajendrasinh Jadeja, Tapankumar Trivedi and Jaymit Surve. The paper, published in Scientific Reports in 2024, discusses the use of a snake robot with deep learning object detection procedure for detecting victims trapped under the rubble of earthquakes[7]. The robotic device contains a camera, microphone and wireless transmitter that transmit the collected information to a remote control station, which uses artificial intelligence for victim detection.

This research is relevant to this study as it reveals the ability of AI-enabled SAR robots to generate data. It is not enough for the robot just to carry out the physical task of saving a life. In addition, it has to collect information in the form of visuals and sounds, transmit this information through communication technology, and process it using artificial intelligence. Such a system is capable of collecting information about not only the person being saved but also other people, residents, bystanders, rescuers, and even property in the area. This paper therefore forms the basis of the investigation of the legal aspects of privacy, data protection, and cybersecurity, although the main emphasis is placed on the performance of procedure and accuracy of detecting survivors.

The ethical and regulatory issues involved with humanitarian drones have been highlighted in the study titled "Ethical Considerations Associated with 'Humanitarian Drones': A Scoping Literature Review" by Ning Wang, Markus Christen and Matthew Hunt. The study, published in Science and Engineering Ethics, looks into the ethical issues that emerge due to the use of drones in the context of humanitarian work[8]. The authors accept the fact that humanitarian drones may have great utility in disaster and relief scenarios. However, they raise some issues which need to be addressed through ethics and regulation.

[7] Rajendrasinh Jadeja, Tapankumar Trivedi & Jaymit Surve, *Survivor Detection Approach for Post Earthquake Search and Rescue Missions Based on Deep Learning Inspired Algorithms*, 14 Sci. Rep. 25047, 25047–48 (2024).
[8] https://link.springer.com/article/10.1007/s11948-021-00327-4.

This research's contribution to this current study comes in the form of an understanding that the humanitarian intent behind the technology does not invalidate the necessity of privacy and regulation controls. The nature of the situation could make it impossible to employ standard means such as prior notification and informed consent, while the surveillance capabilities of drones can lead to the gathering of information about persons who were never meant to be part of the operation. It is hence necessary to strike a balance between humanitarian technology and privacy, among other issues. However, the research in question addresses the humanitarian use of drones as a whole without touching upon ground SAR robots, artificial intelligence, and the Indian legislation.

One such contribution that was made in a later date and relates humanitarian technology and data protection law is the article written by Rogers Alunge Nnangsope titled "Examining the Applicability of Hard Data Protection Law on Demographically Identifiable Information (DII): The Case of Humanitarian UAV/Drone Images in Malawi." It appeared in the Journal of International Humanitarian Action in 2025[9]. The paper considers whether the existing law on data protection sufficiently covers the information that can be found in humanitarian UAV and drone images.

The research is relevant for this current research since it highlights some of the challenges associated with the application of broad principles of data protection to emergency images. SAR robots and UAVs could gather significant visual data in scenarios in which individuals would be unlikely to be able to exercise control over the collection of their visual data. This means that there would be challenges regarding the issue of identifying individuals, processing of data lawfully, limitation of purposes, data minimization, and storage and usage of collected data. The research, therefore, is relevant for analyzing similar issues within the Indian context. However, the geographies involved are Malawi while the subjects are humanitarian UAV imagery and not SAR robotics using AI.

- **Research Gap**

There are many works indicating how robotics, AI, and drones could help in disaster and compassionate aid efforts. However, they pose a lot of ethical, technological, and legal issues. Battistuzzi et al. have identified privacy, accountability, safety, and trust as important issues in

[9] Rogers Alunge Nnangsope, *Examining the Applicability of Hard Data Protection Law on Demographically Identifiable Information (DII): The Case of Humanitarian UAV/Drone Images in Malawi*, 10 J. Int'l Humanitarian Action 1, 1–5 (2025)

rescue robotics. Jadeja et al. show how SAR robots equipped with AI gather and analyze video and audio information about people in order to find them. Wang et al. discuss ethical and regulatory challenges in using drones for humanitarian aid efforts.

However, there exists an important gap in terms of law in India's context. The existing literature fails to consider the applicability of Article 21 of the Constitution of India, Digital Personal Data Protection Act, 2023, Digital Personal Data Protection Rules, 2025, Information Technology Act, 2000 and Disaster Management Act, 2005 in the case of AI-enabled SAR robotics.

Also, there is a lack of research on the gathering of visual, thermal, audio, and location data, the unintentional gathering of bystander and rescuer data, storage, deletion and reuse of rescue footage, cybersecurity risks, and liability distribution between regulators, operators, manufacturers, AI developers, and service providers. The current paper helps fill these research gaps through an analysis of the legal ability of India to safeguard privacy and data for life saving SAR missions.

STATEMENT OF PROBLEM

The growing deployment of AI enabled SAR robots raises the issue of legal responsibility in cases where such technology fails, causes injuries or damages to property, produces inaccurate results, breaches privacy rights or contributes to erroneous rescue efforts. Considering that SAR activities may engage government institutions, rescue organizations, operators, robot manufacturers, developers of AI systems, software vendors and even cloud computing service providers, the identification of those responsible for potential problems in using SAR robots could prove rather challenging. Despite the fact that the Disaster Management Act of 2005 depends on the responsibility of relevant institutions in disaster management, there is no specific legislation covering AI enabled or autonomous SAR systems. The current study therefore explores whether the existing Indian legal framework sufficiently covers the issues of responsibility and liability, negligence, product liability, duty of care and administrative responsibility as well as privacy, data protection and cybersecurity.

RESEARCH OBJECTIVES:

- Analyzing the allocation of legal responsibilities and liabilities between various public

agencies, disaster management agencies, operators, manufacturers, AI developers, software and cloud service providers responsible for the use of AI based SARs.

- Analyzing how the Disaster Management Act, 2005 and other relevant Indian legislation can help in determining the legal obligations and liability for the use of AI based SARs.

- Analyzing the applicability of various doctrines such as negligence, product liability, duty of care, vicarious liability and administrative liability to harm caused by AI based SARs.

- Designing human centric legal framework for data protection and accountability in AI based SAR operations that includes human oversight, AI transparency, safety and cybersecurity measures, data minimization and privacy protection.

RESEARCH QUESTIONS

1.Who should take responsibility and face liabilities in case the AI-powered search-and-rescue robots fail to deliver expected results, generate wrong outputs, create damages, or gather too much personal data when used during disasters?

2.How effectively do the laws concerning privacy, data protection, cyber law, and disaster management in India regulate the collection, processing for emergencies, storage, security, and secondary usage of personal information collected through AI-powered SAR robots, and does a specialized framework become necessary in this case?

SCOPE AND LIMITATIONS OF THE STUDY

The study looks at the legal aspects surrounding the issues of privacy, security, data protection, accountability, and cybersecurity associated with search and rescue (SAR) missions involving AI technology. This encompasses the use of aerial drones, nanodrones, wheeled, tracked, and bipedal robots that have cameras, thermal imaging, microphones, GPS and communication technology, The research analyzes the gathering, transfer, analysis, storage, access, disclosure, sharing, retention, and destruction of video images, audio data, thermal data, biometric data, and geolocation data regarding victims, witnesses, local residents, and rescuers. Responsibility and liability for AI in SAR missions are also looked at in this research.This research paper will

mainly concentrate on the Indian legal and regulatory system, which includes the Digital Personal Data Protection Act 2023, Digital Personal Data Protection Rules 2025, Information Technology Act 2000, Disaster Management Act, 2005, and Article 21 of the Constitution. The main importance is placed on issues such as emergency processing, data minimization, limitation of purpose, bystander data, biometric data and thermal data, AI classification, footage retention, secondary uses, data sharing, cybersecurity, and deletion post operation. International laws and policy frameworks will be examined merely as a reference for finding the gaps in regulations, but not through a comparative analysis.

The research is carried out using the doctrinal approach based on statutes, government sources, policy and literature. Interviews, surveys, field work and technical testing are not utilized in this research nor does it empirically test the accuracy, reliability, navigation, detection or cybersecurity capability of any particular robotic systems. The rescue operations used in this research are only examples and are not used in order to find the legal liability of any particular organization or individual. This research does not give an exhaustive overview of tort law, criminal law, telecommunications law, defence law, procurement law and any other potentially applicable legal area.

RESEARCH METHODOLOGY

This study adopts a doctrinal legal research methodology. It is based on the qualitative research of primary and secondary legal sources relating to the use of AI enabled search and rescue robots in India. The primary sources include the Constitution of India, particularly Article 21, the Digital Personal Data Protection Act, 2023, the Digital Personal Data Protection Rules 2025, the Information Technology Act, 2000, the Disaster Management Act, 2005, relevant judicial decisions, especially Justice K.S. Puttaswamy (Retd.) v Union of India and applicable government policies, notifications and disaster management guidelines. The secondary sources include journal articles, research papers, reports and scholarly writings on artificial intelligence, robotics, privacy, data protection, cybersecurity, disaster management, responsibility and liability. The study analyses the existing Indian legal framework to determine whether it adequately addresses responsibility, liability, privacy, data-protection and cybersecurity concerns arising from AI enabled SAR robots. It also identifies legal and regulatory gaps and suggests the need for specialised guidelines or a regulatory framework that protects individual rights while allowing the effective use of technology in emergency rescue

operations.

LEGAL AND REGULATORY CHALLENGES OF AI-ENABLED SEARCH AND RESCUE ROBOTICS IN INDIA

- **Legal Responsibility for AI Enabled SAR Robots**

The first legal problem relates to who will be held responsible for malfunctioning or damages caused by the AI enabled SAR robot. In as much as a robot lacks a distinct legal entity, responsibility shall be assigned to any of those individuals or bodies involved in designing, procuring, operating, supervising, maintaining, and controlling the robot. This list includes the National, State, and District Disaster Management Authorities, National Disaster Response Force, armed forces, local authorities, incident commanders, robot operators, manufacturers, AI and software developers, cloud services providers, among others.

According to the Disaster Management Act 2005, the policies, plans, and guidelines for disaster management are developed by the National Disaster Management Authority, whereas the National Executive Committee assists in the implementation of actions pertaining to disaster management[10]. Hence, a public agency employing robots cannot completely escape liability merely on the grounds that a private firm provided the robots or on account of automation.

Determining responsibility should follow the principles of control, knowledge, legal duty, and ability to prevent damage. The lead rescue authority is responsible for determining when, why, and how the robot is deployed. An operator can be held responsible for operating beyond its designated parameters, ignoring malfunction indications, blindly trusting wrong coordinates from the AI, and disseminating footage from the rescue operation without permission. Manufacturers can be held responsible for faulty hardware, dangerous design, insufficient instructions, or failure to disclose limitations. Developers and providers of AI and software are also responsible for any of those issues[11].

AI cannot be allowed to acquit humans of their responsibilities. The outputs of AI concerning survivor identification, path planning, thermal analysis, and hazard classification should be

[10] The Disaster Management Act, 2005, No. 53 of 2005, § 6, § 10, Acts of Parliament, 2005 (India).
[11] Maaike Harbers, Joachim de Greeff, Ivana Kruijff-Korbayová, Mark A. Neerincx & Koen V. Hindriks, *Exploring the Ethical Landscape of Robot-Assisted Search and Rescue*, *in* A World with Robots: International Conference on Robot Ethics: ICRE 2015, at 93 (Maria Isabel Aldinhas Ferreira et al. eds., Springer 2017).

considered decision support tools and not the actual decisions themselves. Human supervision is required in those cases[12].

- **Legal Liability for Wrongful Harm**

Responsibility is the obligation to regulate, oversee, and be in charge of using care, and liability is the legal implications of failing in one's responsibility. Liability can occur if the AI-assisted Search & Rescue (SAR) robot inflicts any physical, informational, and privacy injury on a person. Examples of such harm include the robot colliding with someone, misidentifying an object, failing to find a victim, sending false location details, collecting too much personal information, releasing rescue video footage, or cyber attacking the rescue effort[13].

Civil liability may occur due to negligence when a duty of care is not fulfilled and there is harm caused. Liability on the part of a rescue agency can arise due to its failure to test the robot before using it in a dangerous situation without proper supervision, safety measures, and ability to shut it down during an emergency. A producer may be held liable for any defect in the hardware used, battery failure, problems with sensors, or lack of proper warning. An AI designer may be held liable for producing biased results because of the design that does not consider the environmental conditions.

Information Technology Act 2000 may cover unauthorized access, any damage to computer systems, data theft, computer contamination or lack of due security measures[14]. However, it does not cover autonomous SAR robots. The Disaster Management Act ensures that any action taken in good faith cannot be prosecuted[15]. Nevertheless, it should not offer protection against any negligence, wilfulness, recklessness, violation of privacy that could have been avoided, or breach of required safety standards. Hence, guidelines regarding SARs must establish responsibility of all parties concerned.

- **Privacy Implications of SAR Robotics**

There are many privacy issues that arise due to AI enabled search and rescue robots since they

[12] Linda Battistuzzi, Carmine Tommaso Recchiuto & Antonio Sgorbissa, *Ethical Concerns in Rescue Robotics: A Scoping Review*, 23 Ethics & Info. Tech. 863, 863–65 (2021).
[13] Roger Clarke, *The Regulation of Civilian Drones' Impacts on Behavioural Privacy*, 30 Computer L. & Sec. Rev. 286, 296–301 (2014).
[14] Information Technology Act, 2000, No. 21 of 2000, §§ 43, 43A, 66, Acts of Parliament, 2000 (India).
[15] The Disaster Management Act, 2005, No. 53 of 2005, § 73, Acts of Parliament, 2005 (India).

can gather vast amounts of data through their cameras, microphones, thermals and GPS systems during their rescue operations. The fact is that this information can be collected when people are injured, trapped, unconscious, or in any other state that does not allow them to control the gathering of their personal information. The cameras may take pictures of faces, bodies, injuries, homes, private property, and movement of both victims and the ones helping them.

Privacy was recognized by the Supreme Court as a Fundamental Right under Article 21 of the Indian Constitution in K.S. Puttaswamy (Retd.) v. Union of India[16]. Privacy can only be infringed upon by the State in accordance with legality, legitimacy of purpose, proportionality and procedural propriety[17]. It is a legitimate State purpose to save lives or undertake disaster relief operations. But the legitimacy of the purpose cannot allow unlimited surveillance, unnecessary data collection and unknown retention of the rescue data[18].

The proportionality doctrine takes on a lot of significance in the disaster events. The SAR robot might document the collapsed tunnel, flooded place, or the damaged building when it is required to find out any victims or hazards. But the robot must capture only the data which is required for its function. In other words, if thermal images can detect any human presence, there is no need for high resolution images of the face. Live video capturing for rescue operations should not be stored for any commercial or non commercial use without any further reason[19].

- **Data Protection Obligations**

The responsibility to protect data will only be triggered if the data gathered from the SAR robot equipped with AI technology is recorded, transmitted, stored, analyzed, shared or otherwise processed in digital form. Personal data, as used under the Digital Personal Data Protection Act, 2023 (DPDP Act), refers to data that relates to an identifiable individual, whereas processing is defined to include any operation on personal information, whether or not it is automated, such as collection, recording, storage, use, disclosure, restriction, or destruction of

[16] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[17] Justice K.S. Puttaswamy v. Union of India (Aadhaar), (2019) 1 S.C.C. 1 (India).
[18] Roger Clarke, *The Regulation of Civilian Drones' Impacts on Behavioural Privacy*, 30 Computer L. & Sec. Rev. 286, 296–301 (2014).
[19] Rogers Alunge Nnangsope, *Examining the Applicability of Hard Data Protection Law on Demographically Identifiable Information (DII): The Case of Humanitarian UAV/Drone Images in Malawi*, 10 J. Int'l Humanitarian Action 1, 1–5 (2025).

data[20].

The DPDP Act enables data processing based on consent and legitimate purposes. Under Section 7(h), data processing can be done in situations that involve the protection of an individual from danger or emergencies involving the failure of public order. It is crucial because the individual may not have the capacity to give consent as he might be trapped, injured, or unconscious. Nevertheless, data processing for emergency purposes cannot be unlimited[21].

The responsibilities of a Data Fiduciary under Section 8 include being responsible for any processing carried out by itself and by a Data Processor. It shall put in place appropriate technical and organizational measures, have reasonable security safeguards, have redress mechanisms for grievances, respond to data breaches, and delete data once the purpose has been achieved unless required by law[22]. For SAR operations, the lead rescue agency can be considered a Data Fiduciary since it decides on the reasons and methods of collecting the data.

The rescue data is to be utilized solely for the purpose of finding out the survivors and for risk assessment and operation coordination. The rescue data must not be reused for purposes like advertisement, entertainment, irrelevant surveillance, publishing news, AI training or any other kind of information disclosure. The rescue organizations need to frame data policies in writing[23].

- **Cybersecurity and Regulatory Gap**

AI-Based Search and Rescue (SAR) operations face the problem of cybersecurity because any form of cyberattacks may lead to operational errors, data breaches, privacy infringement and put human lives at risk. The use of wireless communication, cameras, sensors, GPS system, software applications of the control center, cloud computing and AI processing makes SAR robots susceptible to hacking attempts, live video interception, GPS manipulation, faulty inputs for sensors, communication disruption, artificial intelligence output interference, rescue video

[20] Digital Personal Data Protection Act, No. 22 of 2023, § 2, Acts of Parliament, 2023 (India).
[21] Digital Personal Data Protection Act, No. 22 of 2023, § 7(h), Acts of Parliament, 2023 (India).
[22] Digital Personal Data Protection Act, No. 22 of 2023, § 8, Acts of Parliament, 2023 (India).
[23] Ministry of Electronics & Information Technology, Notification No. G.S.R. 843(E) (Nov. 13, 2025) (India).

theft and denial of service attacks[24].

The Information Technology Act, 2000 offers general safeguards against unauthorized access, copying or extraction of information, computer contamination and disruption of computer systems. The provisions under Sections 43, 66, 66C, 66E, 72 and 72A can be applicable to cyber crimes if they relate to offences relating to computers, identity theft, privacy violation, confidentiality breach or unauthorized disclosure. However, there is no specific safety and cybersecurity regime available under this Act for AI driven rescue robots[25].

It is therefore important that rescue organizations and technology suppliers embrace privacy by design and security by design initiatives[26]. These include encryption, multifactor authentication, role based access control, software patching, vulnerability assessment, network segmentation, tamper proof auditing, an emergency stop mechanism, backup communication channels, and security audits. For each search and rescue mission, there must be a data governance log capturing the platform utilized, personnel operating the system, data captured, legal justifications for data processing, and recipients.

FINDINGS:

- AI based SAR robots gather detailed personal information such as visuals, sounds, temperatures, biometrics and location data about the victims, observers, residents and rescuers.

- There is no legal framework regarding AI enabled SAR robotics in India. While there exist general laws that could provide an overall legal basis, there is no framework to cover the issues of autonomy, AI errors, malfunction of the robots and liability.

- The robot cannot be held responsible. Responsibility has to be allocated among public bodies, agencies dealing with disasters, operators, manufacturers, AI engineers, software providers, and technology providers considering their degree of control,

[24] Roger Clarke, *The Regulation of Civilian Drones' Impacts on Behavioural Privacy*, 30 Computer L. & Sec. Rev. 286, 296–301 (2014).
[25] Information Technology Act, 2000, No. 21 of 2000, §§ 43, 66, 66C, 66E, 72, 72A, Acts of Parliament, 2000 (India).
[26] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, art. 25, 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).

responsibility, knowledge and ability to prevent the damage.

- Human intervention will still be necessary. AI results related to survivor identification, threat evaluation, route selection and thermal analysis have to be used as secondary tools and subject to adequate supervision.

- Article 21 privacy provisions apply to SAR data gathering. The principles of legality, legitimate purpose, necessity, balanced and procedural safeguards are still applicable in emergency situations.

- Section 7(h) of DPDP Act, 2023 provides a basis for limited emergency processing in times of disaster, but this cannot be relied upon to allow unlimited collection, retention, dissemination, or reuse of rescue data.

- The existing cyber security framework is a generic one and is not changed to SAR operations. The IT Act and CERT-In guidelines do give a framework of cyber security however, there is a need for a framework specifically designed to cover specific risks like GPS spoofing, interference with AI output, interception of communications, and compromise of rescue footage.

- A coordinated accountability framework is needed that includes responsibility matrices, delegation of duties, human intervention, privacy considerations, data governance, security by design, audits, and appropriate NDMA guidelines or SOPs.

CONCLUSION

In this paper, the privacy, protection of personal data, accountability, liability and cyber security implications of using Artificial Intelligence (AI) enabled search-and-rescue (SAR) robots in India were studied. The research succeeded in meeting its objective through analyzing the ability of the Indian constitutional framework, data protection law, cyber law and disaster management to control data collection and processing in SAR operations.

According to this research, the use of Artificial Intelligence (AI) enabled SAR robots can greatly enhance disaster response through cameras, thermal sensors, microphones, GPS and AI analysis which will help in finding the victims, identifying any hazards and performing in difficult terrains. On the other hand, these technologies can collect visual, audio, biometric,

thermal and location data regarding the victims, locals, spectators and rescuers.

Their use is hence associated with legal issues that go beyond operational efficiency.The study indicates that robots cannot be individually responsible from a legal perspective. Legal responsibilities and liabilities must, on the other hand, be apportioned between governmental agencies, disaster management authorities, operators, manufacturers, artificial intelligence developers, software companies, cloud service providers, and communication companies depending on the degree of control, harm. Liability could result from failure of equipment, malfunctioning of artificial intelligence products, negligence of operators, insufficient human monitoring, disclosure without consent, and cybersecurity threats.

Article 21 and the privacy principles of Puttaswamy further indicate that processing must be lawful, legitimate, necessary, proportional, and safeguarded procedurally[27]. Section 7(h) of the Digital Personal Data Protection Act, 2023 allows emergency processing for protection or assistance of individuals in cases of disasters, but not unlimited data processing, storage, and disclosure for unrelated purposes[28].

In summary, the research shows that the law in India is important as a base but is incomplete when it comes to SAR robotics. The best solution to adopt would be to build on the current laws using the guidelines of the NDMA, SOPs, procurement conditions, responsibility matrices, human supervision, minimization of data and cybersecurity measures[29].

SUGGESTION

The study suggests that India should regulate AI enabled search and rescue robots by implementing the existing legal framework. First, the National Disaster Management Authority should formulate guidelines, as per Section 6 of the Disaster Management Act, 2005, and integrate them into the National, State and District Disaster Management Plan. This will involve making a responsibility matrix on paper prior to each rescue operation, which states who is responsible for procurement, testing, operation, supervision, maintenance and cybersecurity. The lead agency for the rescue mission should be considered the Data Fiduciary as per Section 8(1) of the DPDP Act, 2023, while the manufacturers, AI developers and cloud

[27] Justice K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
[28] Digital Personal Data Protection Act, No. 22 of 2023, § 7(h), Acts of Parliament, 2023 (India).
[29] The Disaster Management Act, 2005, No. 53 of 2005, § 6, Acts of Parliament, 2005 (India); Information Technology Act, 2000, No. 21 of 2000, §§ 43, 66, 66C, 66E, 72, 72A, Acts of Parliament, 2000 (India).

service providers can be involved as Data Processors as per Section 8(2)[30].

Secondly, use of outputs from the AI system for survivor detection, dangers and route selection must be considered decision support at best, with such decisions to be verified and overridden if necessary by the human operator, and logged in a mission report detailing all of the decisions made by the AI and the human operator. Section 73 of the Disaster Management Act should provide immunity only when decisions were made in good faith, as evidenced by proper completion of testing, oversight and data governance responsibilities[31].

Thirdly, in light of Articles 21 and Puttaswamy, any processing of data under Section 7(h) of the DPDP Act must be confined to locating survivors, risk assessment and rescue coordination, and include principles of data minimization, deletion post operation and non use for public relations, unrelated surveillance or AI training. Further, it must also mandate the mandatory data security and data breach notification measures required under Sections 8(5) and 8(6) of the DPDP Act, the Information Technology Act, 2000 and CERT-In directions, and hold vendors accountable to it through contracts[32].

[30] The Disaster Management Act, 2005, No. 53 of 2005, § 6, Acts of Parliament, 2005 (India); Digital Personal Data Protection Act, No. 22 of 2023, § 8(1)-(2), Acts of Parliament, 2023 (India).

[31] The Disaster Management Act, 2005, No. 53 of 2005, § 73, Acts of Parliament, 2005 (India).

[32] Digital Personal Data Protection Act, No. 22 of 2023, §§ 7(h), 8(5)-(6), Acts of Parliament, 2023 (India); Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); Information Technology Act, 2000, No. 21 of 2000, §§ 43, 66, 70B, Acts of Parliament, 2000 (India).