BALANCING AI INNOVATIONS RELATED TO AUTOMATED VEHICLES AND THEIR PRIVACY RIGHTS

R.Saaishri, Sastra University

ABSTRACT

As nations strive to protect individual privacy while fostering technological advancement, establishing a balance between AI innovation and privacy rights has become a critical issue. This research paper majorly contrasts the General Data Protection Regulation (GDPR) of the European Union, the Protection of Personal Information Act (POPIA) of South Africa, and other related laws with India's Digital Personal Data Protection Act (DPDPA). Although these laws aim to regulate data protection, the DPDPA faces unique challenges due to its recent implementation and the evolving digital landscape. The GDPR is widely regarded as the gold standard, offering robust protections like the right to be forgotten and explicit consent requirements, ensuring strong user control over personal data. Similarly, POPIA grants extensive rights to data subjects and emphasizes the lawful processing of personal information. In contrast, while the DPDPA marks significant progress for India, it has drawn criticism for its broad exemptions for government agencies, which may undermine the right to privacy. AI and data privacy are closely intertwined, as AI systems often rely on vast amounts of personal data to function effectively. Despite AI's potential to revolutionize industries and enhance lives, it raises serious privacy concerns. The collection, processing, and storage of personal data by AI systems can lead to misuse, security breaches, or unauthorized access, compromising user privacy. To maintain trust and protect privacy in an increasingly digital world, it is crucial that AI development adheres to stringent data protection principles, such as minimizing data collection, securing user consent, and implementing robust anonymization techniques. India's legal framework presents both advantages and disadvantages when compared to the laws of other nations. While the DPDPA offers mechanisms for redressing data breaches and protecting privacy rights amidst rapidly advancing AI, its broad data localization requirements and limited accountability mechanisms raise concerns about stifling innovation and complicating international compliance. This research paper will explore the current challenges, assess whether these laws provide effective remedies, and evaluate where India stands in comparison to other countries in case of automated vehicles.

INTRODUCTION

The transportation sector is experiencing profound shifts as an effect of the rapid growth of artificial intelligence (AI) in the field of automated vehicles, which holds the promise of increased convenience, safety, and efficiency. But these advancements also bring a significant challenge in defending the right to privacy of those whose data is collected, analyzed, and used by these cars. Robust regulatory frameworks are necessary to ensure responsible handling of the large volumes of personal data involved, which include biometric data, driving patterns, and geolocation.

Three comprehensive legislative attempts to protect privacy in a world increasingly driven by data are the Protection of Personal Information Act (POPIA) in South Africa, the Digital Personal Data Protection Act (DPDPA) in India, and the General Data Protection Regulation (GDPR) of the European Union. There are provisions in each of these laws designed to guarantee accountability, openness, and consent in the collection and processing of personal data.

This article examines how concerns regarding privacy raised by AI advancements in automated vehicles are addressed by the GDPR, DPDPA, and POPIA. It focuses on important issues like data minimization, consent, data sharing, and accountability while examining the potential conflicts and opportunities between fostering innovation in this area and upholding strict data protection regulations. We seek to understand how these legal frameworks can support a balanced approach to technological advancement and privacy rights by evaluating their advantages and disadvantages.

RESEARCH METHODOLOGY: COMPARATIVE ANALYSIS AND DOCTRINAL RESEARCH

Comparative analysis and doctrinal research on the 3 legislations of the European union, South Africa and India.

RESEARCH PROBLEM: Despite the rapidly evolving automobile industry, there are inadequate provisions governing data breaches and privacy violations in automated vehicles.

RESEARCH QUESTION:

1: What are the privacy vulnerabilities that exist in automated vehicles?

2: How do different countries' legislation address privacy issues?

TYPES OF VEHICLES[1]

Level 0: No driving automation

Most cars on the road today are manually operated, or Level 0. The "dynamic driving task" is performed by humans, even though there might be systems in place to assist the driver. An illustration of this would be the emergency braking system, which does not fall under the automation category because it does not, in theory, "drive" the car.

While the vehicle is fitted with a system that offers brief driving assistance, like warning signals or emergency safety actions, the driving experience is still fully within the driver's control. As a result, the driver is in charge of operating the vehicle and keeping an eye out for any potential alerts or safety procedures. This includes applying the brakes, steering, and acceleration.

Level 1: Assistance for Drivers

The least amount of automation is this one. The car has a single automated system that helps the driver with tasks like accelerating and steering (cruise control). Because the human driver is in charge of steering and braking in addition to keeping the car at a safe distance behind the next car, adaptive cruise control is considered a Level 1 feature.

The following are a few instances of technologies found in Level 1 cars:

Lane-keeping assistance, lane-centering assistance, adaptive cruise control, or electronic adaptive speed regulator

Level 2: Partial driving automation

This refers to ADAS or advanced driver assistance systems. The car is capable of steering as well as accelerating or decelerating. Because a human is seated in the driver's seat and can take control of the vehicle at any time, this automation falls short of being fully autonomous. Level 2 systems include Cadillac's Super Cruise and Tesla Autopilot from General Motors.

Level 3: Conditional driving automation

When the driver gives the system permission to take over, Level 3 offers conditional driving automation functions, putting us unquestionably at a more advanced level that is not yet widely available in the market. In simple terms, this means that the driver must be seated in the driver's

[1] B. C. Zanchin, R. Adamshuk, M. M. Santos and K. S. Collazos, "On the instrumentation and classification of autonomous cars," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 2017, pp. 2631-2636, doi: 10.1109/SMC.2017.8123022.

seat and prepared to take over when needed or requested, even though the system performs all driving functions when it is activated.

Level 4: High driving automation

The primary distinction between Level 3 and Level 4 vehicles is that the latter's systems have the capability to take action in the event of a malfunction without the driver having to get involved. Nonetheless, the driver retains the ability to manually take control of the car.These vehicles are only permitted to be used under very specific and well-defined conditions according to current regulations, such as in city centers with very low speed limits. They are therefore typically intended for use on ride-sharing vehicles.

Level 5: Full automation of driving

According to SAE classification, Level 5 vehicles use the most advanced technologies, enabling them to reach the highest level of automation.

Indeed, regardless of the driving situation or the condition of the roads, they don't even need manual intervention in an emergency. For this reason, there are no pedals or steering wheels on the vehicles. As a result, someone could board and engage in any activity while completely disregarding the driving environment.

COLLECTION OF DATA IN THESE VEHICLES

Automated vehicles, which depend on intricate systems that continuously collect, process, and analyze data in order to function autonomously, are a breakthrough in transportation technology. These cars interpret and navigate their surroundings using a range of sensors, cameras, radars, and GPS technologies. They collect information about their environment with these tools, including traffic signals, surrounding cars, pedestrians, and road conditions. Real-time decision-making made possible by this data enables the car to steer, brake, change course, and adjust speed in order to avoid traffic jams or other obstacles.

Automated cars gather a ton of data about users in addition to environmental indicators. For example, they could keep tabs on a car's whereabouts, observe how its occupant drives, and keep track of past travelogues. Additionally, some cars collect biometric information like voice or facial recognition for driver identification. commands for in-car systems. These features are designed to enhance convenience and personalization, offering users a tailored experience based on their preferences.

For autonomous cars to function properly, a lot of data is needed. Typically, these sensors consist of a GPS unit for navigation, a wheel encoder to track the vehicle's movements, radar units mounted on the front and rear bumpers to detect traffic, and a color camera located next to the rearview mirror.

The cameras raise the most privacy issues, particularly if the data they collect is combined and kept in one place. The use of CCTV surveillance is prohibited in thirteen states in the US, and all states demand appropriate notice. Whereas an automobile's sensors are meant for autonomous driving, CCTV is meant for surveillance. In addition, unlike CCTV, which is limited to a specific area, AVs are free to operate on any public road at any time. A better comparison would be a "dash cam," or dashboard camera, though data gathered by these devices is unlikely to be centralized and processed.[2]

It's unclear if comfort using dash cams or CCTV would translate to comfort using data collected by commercial AV fleets identification; a rotating light detection and ranging (LiDAR) sensor on the roof that creates a three-dimensional (3D) map of the surroundings; and lane departure, read collision, and pedestrian alerts.

With the use of a network of sophisticated sensors, cameras, radar systems, and communication technologies, autonomous vehicles (AVs) gather data. Together, these systems allow the car to sense its surroundings, make decisions, and drive safely without the need for human assistance. In autonomous cars, data is normally gathered in the following ways:

1. Sensors and Cameras: LiDAR (light detection and ranging), ultrasonic, and high-resolution cameras are just a few of the sensors that autonomous cars are outfitted with. These gadgets constantly scan the area around the car, gathering information about the state of the road, obstructions, traffic lights, pedestrians, and other cars. While cameras record visual data to identify road markings, lanes, and signs, LiDAR creates a three-dimensional map of the surrounding area.

2.Radar Systems: Radar systems are employed to measure an object's distance and speed from a moving vehicle. This technology is essential for collision avoidance and adaptive cruise control. It is especially good at identifying moving objects, like other cars or cyclists.

[2] Divya, K., and G. Girisha. "Autonomous car data collection and analysis." *Int. Journal of Scientific Research & Engineering Trends* 7.3 (2021).

3.Inertial Measurement Units (IMUs) and GPS: GPS provides precise location information that helps the car find its place on the road and navigate to its destination. IMUs, which monitor the orientation, acceleration, and motion of the car, work in conjunction with GPS data to provide seamless navigation—even in places with spotty satellite reception.

4.Vehicle-to-Everything (V2X) Communication: V2X technology allows autonomous cars to talk to other cars, infrastructure (such as traffic signals), and even people on foot. By anticipating potential hazards, coordinating traffic flow, and obtaining real-time updates about road conditions, this data exchange enhances traffic management and safety.

5.Internal Systems Monitoring: Information about the internal workings of the car is gathered from a number of onboard systems, including fuel efficiency, tire pressure, battery condition, and engine performance. This operational data guarantees that the car is operating at peak efficiency and can anticipate problems that need to be fixed.

6.Data about User and Vehicle Interactions: Autonomous cars also gather information about user interactions, such as voice commands, in-car preferences, past navigation history, and biometric information (such as fingerprint or face recognition for driver identification). This data enhances the user experience by offering personalized services and ensuring secure vehicle access.[3]

CASES OF DATA BREACH, HACKS OR LEAKS

Several ethical hacking attempts have targeted Tesla vehicles, exposing flaws in their AI-driven systems. These incidents have demonstrated the potential for exploiting connected and autonomous vehicle systems.

1. Model S Hack Tesla (2015)[4]

Security researchers from Keen Security Lab were able to remotely hack a Tesla Model S in 2015. They succeeded in seizing control of a number of important components, including the infotainment system, door locks, mirrors, and brakes. To address the vulnerabilities, Tesla released an over-the-air (OTA) software update very soon after. This hack demonstrated how sophisticated AI systems in cars, which control driving and safety, are vulnerable to cyberattacks.

[3] Henry Alexander Ignatious, Hesham-El- Sayed, Manzoor Khan, An overview of sensors in Autonomous Vehicles,Procedia Computer Science, Volume 198,2022, ISSN 1877-0509,
[4] How to hack a self-driving car Ornes, Stephen 2020/08/01 SN - 0953-8585

2. 2016 Tesla Autopilot Hack[5]:

Researchers at Ben Gurion University and Southwest Jiaotong University conducted a noteworthy incident in which they showed how to manipulate Tesla's AI-powered Autopilot system. They tricked the car's image recognition system by making insignificant changes to road signs (adversarial attacks), which caused the vehicle to misinterpret traffic signs and make potentially hazardous decisions. This demonstrated how indirect attacks on AI systems could compromise their security, prompting questions about the security of autonomous driving systems.

3. Tesla Autopilot and Security Vulnerabilities (2017):

In 2017, scientists from the same Keen Security Lab discovered fresh flaws that once more gave them remote control over a Tesla automobile. They used the Autopilot system this time to activate the steering and acceleration functions. In a timely manner, Tesla addressed these problems by releasing another security patch.

4.Security researchers found several flaws in BMW's connected car systems in 2019 that affected different models. The vulnerabilities were found by Tencent Keen Security Lab, a Chinese cybersecurity company, and they revealed significant risks that could give hackers access to sensitive data and remote control over specific vehicle functions.

BMW's iDrive infotainment system was discovered to be susceptible to intrusions. The navigation system, media, and other functions of the car could be manipulated by hackers.

Updates sent- Over the air (OTA): BMW's OTA update system was one of the weak points. Vehicle control systems could be compromised if a flaw in the procedure was used to introduce malicious code during software updates.

Effect on the Automobile Sector:

Given how much more software and AI-driven features are being incorporated into cars, this incident brought to light the growing significance of cybersecurity in connected vehicles. The flaws highlighted the necessity of strong security measures in contemporary automobiles by revealing how external systems like infotainment and telematics could act as entry points for

[5] OVER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS Sen Nie, Ling Liu, Yuefeng Du, Wenkai Zhang Keen Security Lab of Tencent

hackers.[6]

5. Telematics and Breach of User Data

Via telematics systems, connected cars transmit vast volumes of data to automakers, insurance providers, or outside services. Driving habits, location history, and other private information may be revealed if this data is intercepted or leaked. These breaches impact the larger data ecosystem of smart cars, even though they aren't always AI-specific.

6. Issues with Data Security in Autonomous Vehicles

The integrity of sensor data is a persistent concern because autonomous vehicles (AVs) mainly rely on AI to process and react to this data:

Adversarial Attacks on AI Models: Researchers have demonstrated that subtle changes to input data or road signs can be used to manipulate AI models. For example, a minor alteration to a stop sign could lead to a dangerous misunderstanding by an AI-powered vehicle.

Sensor Spoofing: Using spoofing attacks, hackers can target LIDAR, radar, and camera systems, giving the AI in the car false information that could result in accidents or risky driving practices.[7]

7. The 2019 Mahindra e2o Vulnerabilities

It was discovered that the telematics and connected car systems of the Mahindra e2o, an electric vehicle marketed in India, had security flaws. Hackers may be able to remotely take over specific vehicle functions or access vehicle data, such as user location and driving habits, thanks to these vulnerabilities. The possible risk underscored the need for improved security in India's expanding electric vehicle market, even though no significant breach was reported.

8. Connected Car Vulnerabilities with Tata Nexon

The telematics system of Tata's Nexon, which has a connected car platform, has also been criticized for possible vulnerabilities. Security experts have cautioned that sensitive data, such as user information and vehicle diagnostics, may be exposed in such systems due to inadequate authentication procedures and weak encryption.

---

[6] Zhang, W., Liu, L., & Nie, S. (2019). "Security Assessment of Connected Cars: A Case Study of BMW." *IEEE Transactions on Intelligent Transportation Systems*.

[7] Huang, L., & Wang, Y. (2017). "Adversarial Attacks on Autonomous Driving Systems." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*

Future Risks: Data leaks are becoming more likely as India transitions to more AI-driven, networked, and driverless automobiles. These might include:

Location data: Monitoring the real-time movements of users.

Vulnerabilities that could reveal driving habits, vehicle performance, and other private information are included in vehicle diagnostics.

In ride-sharing or delivery systems where customer data may be compromised, telematics and fleet management are utilized.

9. Vehicle Telematics and API Vulnerabilities

Security experts detected that vulnerabilities in telematics as well as API systems provided illicit access to any vehicle to the brands Acura, Honda, Kia, and Nissan. Hackers then utilize these weaknesses to remote controls the functionality of a vehicle, user information available in a vehicle, and even track the vehicle. For instance, there was vulnerability in SiriusXM's connected vehicle services that gave illegal access to sensitive data and vehicle commands.

PROVISIONS RELATED TO THE ABOVE-MENTIONED ISSUES IN MOTOR VEHICLES ACT 1998

The Motor Vehicles Act, 1988 defines a motor vehicle in Section 2(28) as:[8]

Any mechanically propelled vehicle adapted for use upon roads whether the power of propulsion is transmitted from an external or internal source, and includes a chassis to which a body has not been attached and a trailer; but does not include a vehicle running upon fixed rails or a vehicle of a special type adapted for use only in a factory or in any other enclosed premises or a vehicle having less than four wheels fitted with an engine capacity not exceeding twenty-five cubic centimeters.

The definition encompasses cars, trucks, and buses and many other types of vehicles traveling on public roads.

Exclusion of Self-Driving Vehicles

The definition of automated vehicles does not typically fall under the terms as provided for by the Motor Vehicles Act. It mainly refers to mechanically propelled vehicles, in which a human needs to operate to drive them, while automated vehicles have the capability to drive without

[8] Section 2(28) of the Motor Vehicles Act, 1988

a human's direct control over it.

Important Points About Automated Vehicles:

Lack of Human Operation: The current definition focuses on vehicles that are actually driven by individuals. Automated vehicles, which are self-driving, thus seem to violate this conventional definition. Automated vehicles are mostly vehicles which assist humans for a smooth driving experience . With existing regulations about automated vehicles, it remains to be seen if they fall within the meaning of the current definitions, thus raising potential legal inconsistencies about their use and liability on public roads.

The Motor Vehicles Act, 1988, in India primarily focuses on conventional vehicles and does not directly address the use or regulation of fully automated or autonomous vehicles. However, amendments have been introduced to accommodate advancements in vehicle technology. Here are key points about how the act aligns with automated vehicle technology:

1.Motor Vehicles (Amendment) Act, 2019[9]: This recent amendment includes some indirect provisions that touch on automated vehicles, though it primarily aims to improve road safety, licensing, and penalization for traffic violations. There's acknowledgement of the need for future amendments to regulate autonomous vehicle technology.

2. Testing and Approval: Currently, the Act provides for the regulation of vehicle testing, certification, and approval processes, which may apply to automated vehicle technology. However, comprehensive testing standards specifically for autonomous vehicles are not fully established.

3.Driver Responsibility: The Act mandates that the driver is responsible for operating the vehicle safely, which may conflict with autonomous vehicles that require minimal human intervention. Future provisions may need to address the concept of "driver" responsibility in vehicles that operate without direct human input.

4. Insurance and Liability: The Act specifies the responsibility of drivers and owners in cases of accidents, but it doesn't yet define liability when it comes to autonomous vehicles, especially in cases where a system malfunction or software failure is involved.

5.Data and Privacy Concerns: While not directly in the Motor Vehicles Act, autonomous vehicles raise data privacy concerns, as these vehicles rely on data collection and GPS tracking.

[9] Motor Vehicles (Amendment) Act, 2019

In the future, alignment with the Digital Personal Data Protection Act (DPDPA) may be required to address privacy and data security concerns.

GENERALIZED COMPARISON ON THE DATA PROTECTION LEGISLATIONS OF DIFFERENT COUNTRIES

LAWS THAT REGULATE THE PRIVACY OF INFORMATION IN INDIA

Privacy legislation to govern the data leaks or breaches in India

IT ACT

The IT Act is the primary legislation governing data privacy and security in India. Key provisions related to data breaches include:

Section 43A:[10] This section holds organizations liable if they fail to implement reasonable security practices to protect sensitive personal data, leading to data breaches. Affected individuals can claim compensation for damages.

Section 66:[11] Provides penalties for unauthorized access, hacking, and data theft, including imprisonment and fines.

Section 72A[12]: Penalizes disclosure of personal data without consent, even when such information is obtained legally by someone in their professional capacity.

DIGITAL PERSONAL DATA PROTECTION ACT

1. Data Breach Notification Requirement

Section 9(3)[13] of the DPDPA mandates that data fiduciaries (organizations handling data) must report any data breach to both the Data Protection Board of India and affected individuals.

The breach notification should be made as soon as possible and must include information on the nature of the data breach, its likely consequences, and the remedial steps taken.

This provision aims to ensure transparency in the event of a data breach and helps mitigate the effects by allowing individuals to take appropriate action.

[10] Section 43A of Infromation technology act 2000
[11] Section 66 of infromation technology act 2000
[12] Section 72A of infromation technology act 2000
[13] Section 9(3) of the Digital Personal Data Protection Act, 2023

2. Accountability of Data Fiduciaries

Data fiduciaries are required to implement appropriate security safeguards to protect personal data, including encryption, access controls, and other technical and organizational measures. Failure to do so can lead to penalties.

If a data breach occurs due to negligence in implementing these measures, the organization can be held accountable and face severe penalties.

3. Penalties for Data Breaches

The DPDPA imposes heavy penalties for failing to report a data breach or for inadequate protection of personal data.

The maximum penalty for a data breach or non-compliance can be up to ₹250 crore (approximately $30 million), depending on the severity of the breach and the extent of harm caused.

4. Rights of Data Principals (Individuals)

If a data breach affects personal data, the affected individuals (referred to as data principals) have the right to be informed about it.

Individuals can seek redress for the harm caused due to the breach through the Data Protection Board.

5. Role of Data Protection Board of India

The Data Protection Board is empowered to take action in cases of data breaches. It can investigate breaches, order compensation to individuals, and impose penalties on organizations found violating data protection obligations.

PRIVACY LEGISLATION RELATED TO DATA LEAKS OR BREACH IN SOUTH AFRICA

The Protection of Personal Information Act (POPIA), enacted in South Africa, sets out rules for handling personal data to protect the privacy of individuals. It includes provisions to address data leaks and ensure data security. Here's how POPIA addresses data breaches:

1. Obligations to Notify in the Event of a Data Breach

Section 22[14] of POPIA mandates that, in the event of a data breach, the responsible party (data

[14] Section 22 of Protection of Personal Information Act

controller) must notify:

The Information Regulator (South Africa's data protection authority).

The affected data subject (the individual whose data has been compromised).

The notification must be done as soon as reasonably possible, after the discovery of the breach, to allow individuals to take protective measures.

2. Contents of the Data Breach Notification

The breach notification must include:

The nature of the data that was compromised.

Recommendations to the data subject on how to mitigate the potential impact.

The measures being taken by the responsible party to address the breach.

If necessary, details on how the data subject can obtain further information about the breach.

3. Data Security Requirements

Section 19[15] of POPIA requires responsible parties to implement appropriate and reasonable technical and organizational measures to secure personal data from loss, damage, and unlawful access.

These measures should be aligned with the sensitivity of the personal data processed and the potential impact of a breach.

4. Penalties for Non-compliance

Failure to comply with POPIA's data protection requirements, including failure to notify data subjects or regulators about a data breach, can result in penalties.

Administrative fines can go up to 10 million ZAR (approximately $550,000), and, in extreme cases, criminal charges can result in imprisonment of up to 10 years.

5. Rights of Data Subjects

Individuals affected by a data breach have the right to be informed about it promptly. They can take action to protect themselves or seek redress if the breach results in harm.

[15] Section 19 of Protection of Personal Information Act

Data subjects also have the right to lodge a complaint with the Information Regulator if they believe their data has been mishandled.

6. Remedial Measures

POPIA encourages responsible parties to adopt a proactive approach, such as encrypting data and conducting regular security assessments, to prevent breaches and minimize risks.

Summary

POPIA's provisions ensure that data controllers have clear obligations in the event of a data leak, emphasizing quick reporting, adequate security measures, and accountability. The law strengthens the rights of individuals to be informed about and mitigate the effects of a data breach.

PRIVACY LEGISLATIONS RELATED TO DATA BREACH OR LEAKS IN EUROPEAN UNION

The General Data Protection Regulation (GDPR) is the EU's comprehensive law on data protection and privacy. It includes several key provisions addressing data leaks (or breaches) and privacy rights. Here's a breakdown of GDPR's relevant sections:

1. Obligation to Notify in Case of Data Breach

Article 33[16]: This mandates that data controllers (organizations processing personal data) must notify the supervisory authority (data protection regulator) within 72 hours of becoming aware of a personal data breach, unless the breach is unlikely to result in a risk to the rights and freedoms of individuals.

The notification must describe:

- The nature of the breach.
- The categories and approximate number of data subjects affected.
- The likely consequences of the breach.
- Measures taken or proposed to mitigate its effects.

Article 34[17]: If the data breach poses a high risk to the affected individuals, the data controller must also inform those individuals directly and without undue delay. This allows individuals

[16] Article 33 of General Data Protection Regulation
[17] Article 34 of General Data Protection Regulation

to take steps to protect themselves.

2. Data Security Obligations

Article 32[18] Requires data controllers and processors to implement appropriate technical and organizational measures to secure personal data, including:

- Encryption.

- Pseudonymization.

- Regular testing of security measures.

- Risk assessments to ensure security in data processing.

- This article emphasizes the need for data minimization and privacy by design, meaning that privacy considerations should be embedded into the development of technologies and services from the outset.

3. Penalties for Data Breaches

Under Article 83[19] non-compliance with GDPR's provisions, including failure to adequately protect personal data or report a data breach, can result in substantial fines:

Up to €10 million or 2% of global annual revenue, whichever is higher, for failures related to breach notification.

More severe breaches of core data protection principles can attract fines of up to €20 million or 4% of global annual revenue.

4. Data Subjects' Rights

GDPR grants individuals (data subjects) various rights in relation to their personal data:

Right to be informed (Articles 12-14[20]): Data subjects must be informed about data collection, processing, and any breaches affecting their data.

Right to access and rectification (Articles 15-16[21]): Individuals can request access to their personal data and request corrections if inaccurate.

[18] Article 32 of General Data Protection Regulation
[19] Article 83 of General Data Protection Regulation
[20] Article 12-14 of General Data Protection Regulation
[21] Article 15-16 of General Data Protection Regulation

Right to erasure (right to be forgotten)(Article 17[22]): Individuals can request the deletion of their personal data under certain circumstances, especially if the data is no longer needed for its original purpose.

Right to restrict processing (Article 18[23]) and Right to data portability(Article 20[24]): Individuals have control over how their data is processed and can request their data in a structured format.

5. Accountability and Record-Keeping

Under Article 30[25], data controllers must maintain records of all processing activities and be able to demonstrate compliance with the GDPR principles (e.g., transparency, security, and minimization).

Data Protection Impact Assessments (DPIA) are required for high-risk processing activities to identify risks to data privacy and security and implement appropriate safeguards.

6. Role of Data Protection Officers (DPOs)

Under Articles 37-39[26], organizations that handle sensitive data or process large amounts of personal data must appoint a Data Protection Officer (DPO)to monitor compliance with GDPR, conduct audits, and act as a point of contact for the supervisory authority.

DIGITAL PERSONAL DATA PROTECTION Act (DPDPA) ITS DRAWBACKS COMPARED WITH GENERAL DATA PROTECTION REGULATION ACT (GDPR) AND PROTECTION OF PERSONAL INFORMATION ACT (POPIA)

1.Govt power to exempt itself, demand information from companies, and retain data.

The DPDP Bill gives the government the authority to notify any of its agencies that they are exempt from the Bill for reasons such as maintaining public order or ensuring state security. To put it another way, any government agency that is exempt from the DPDP act is free to gather and use citizens' personal information for any reason they choose, without first having to adhere to any of the protections outlined in the bill. Furthermore, Section 36[27] gives the government the authority to request personal information from private businesses "for purposes

[22] Article 17 of General Data Protection Regulation
[23] Article 18 of General Data Protection Regulation
[24] Article 20 of General Data Protection Regulation
[25] Article 30 of General Data Protection Regulation
[26] Article 37-39 of General Data Protection Regulation
[27] Section 37 of The Digital Personal Data Protection Act (DPDPA)

of this Act," a phrase that is not further explained. These two clauses, along with the government's unrestricted ability to keep personal information for as long as it takes, without regard to whether the intended use has been fulfilled, mean that the government has a carte blanche to carry out mass surveillance. Furthermore, there is an automatic exemption for processing personal data for the prevention, investigation, etc., of crime, without the need for the government to issue any notification.

POPIA explicitly provides exemptions for governmental bodies, while GDPR applies uniformly without specific exemptions but allows for national restrictions under certain conditions.

The government is expressly permitted to exempt itself from compliance under specific provisions of POPIA. The following are important factors:

Explicit Exemptions: Section 3(1)(b)[28] of POPIA declares that it does not apply to the processing of personal data by the state while it is carrying out a duty required for the administration of justice, law enforcement, or any other governmental function. This enables the government to handle data without being constrained by certain private entity protections.

Conditions for Exemption: Nevertheless, the government is still subject to the legality, reasonableness, and necessity principles when processing personal data, even if it chooses to exempt itself. This implies that even though some duties might be dropped, the general objectives of safeguarding personal data are still a priority

GDPR, on the other hand, does not specifically contain any clause that would let the government avoid fulfilling its obligations. Important points consist of:

Uniform Application: GDPR ensures a uniform approach to data protection across all sectors by applying to all entities, including governmental bodies. This implies that when processing personal data, government agencies must follow the same stringent guidelines as private businesses.

Limited National Exceptions: Although GDPR is a uniform law, member states may enact laws restricting data processing for public safety, law enforcement, and national security reasons under Article 23[29]. Any such limitations, though, have to be reasonable, required, and

[28] Section 3(1)(b) Protection of Personal Information Act
[29] Article 23 of General Data Protection Regulation

considerate of fundamental rights. This permits national laws to alter how GDPR applies in particular situations, but it does not amount to an exemption.

2. Free pass for scraping of publicly shared personal data

Clause 3(c)(ii) of the act allows companies to process publicly shared personal data without consent or adhering to other provisions, allowing AI services like OpenAI's ChatGPT and Google Bard to scrape data without any consent, and raises possibilities for facial recognition tools using publicly available profile photos.

In summary, while both POPIA and GDPR acknowledge the processing of publicly shared personal data, they differ significantly in their approach to consent, data subject rights, and enforcement mechanisms. POPIA's provisions may provide broader leeway for processing without consent, whereas GDPR emphasizes individual rights and stricter accountability measures.

No consent is required for sharing data with others: When obtaining consent, a company does not have to disclose who all the data will be shared with and for what purposes.

Both POPIA and GDPR would forbid a business from sharing data in your situation without authorization or without alerting all parties involved of the purpose of the sharing. Although they stress the value of openness and informed consent, GDPR has stricter regulations and clearer guidelines for consent and data sharing.

SUGGESTIONS

Licensing and Certification: Introduce specialized licensing or certification processes for vehicles with higher automation levels, especially Levels 3 and above. This may include specific approvals for software systems, machine learning algorithms, and data security measures.

Emergency Manual Override: Mandate the inclusion of manual override functions in AVs to allow human intervention during system failures or emergencies, particularly for Levels 3 and 4 automation.

Post-Accident Reporting and Data Retention: Create protocols for data recording during incidents, including collision event data and system status records, to investigate faults accurately. This aligns with the DPDP Act's requirements for data transparency and access controls.

Data Minimization: Limit data collection to essential information only. AVs generally collect data for navigation, decision-making, and user preferences. Under the DPDP Act, AVs should only collect the minimum data needed for these purposes to ensure compliance.

User Consent and Transparency: Automated vehicle systems should obtain user consent for data collection, specifying which types of data will be collected, the purpose, and duration of storage. In line with DPDP guidelines, this should be communicated in simple language at the point of interaction with the AV's system.

Data Storage and Processing Boundaries: Define protocols for data storage, processing, and transfer. Given that AVs rely on sensitive data, such as real-time location and personal habits, storage must be encrypted, anonymized where feasible, and retained only for a limited duration.

Access Control and User Rights: AV users should have the right to access, correct, or delete their data. Provisions under the DPDP Act allow users to exercise control over their personal data, meaning AV systems should incorporate user-friendly options for data management.

Third-Party Data Processing: For AVs that use third-party services (e.g., cloud storage, mapping software), clear protocols should outline third-party responsibilities and ensure compliance with DPDP requirements.

Independent Regulatory Body for AV Compliance: Establish an autonomous regulatory body to oversee AV compliance with both the MV Act and DPDP Act. This body would work closely with manufacturers, government agencies, and cybersecurity experts to address emerging challenges in AV technology and data security.

Ethics and Transparency in AI Decisions: Ensure that decision-making algorithms in AVs are auditable and ethically sound, especially regarding situations where AVs may need to make decisions impacting human safety.

Integration with Data Protection and Transport Authorities: Regular coordination between bodies such as the Ministry of Road Transport and Highways and the Data Protection Authority under the DPDP Act will ensure comprehensive oversight of AVs, covering both transport regulations and data privacy.

Inclusion of Provisions in Information Technology Act:inclusion of clauses limiting how much data businesses can use. Even though customers have given businesses permission to use their data, businesses should only use specific data, obtain permission again, and clearly define how the data will be used.

CONCLUSION

In conclusion, the intersection of automated vehicle (AV) innovations and data privacy legislation presents complex challenges across GDPR, DPDPA, and POPIA frameworks. AVs, heavily reliant on data collection and processing, raise significant privacy concerns, particularly regarding real-time location tracking, behavioral data, and personal information. GDPR's strict data protection guidelines, including data minimization and user consent, prioritize individual privacy rights in the EU. In contrast, India's DPDPA balances user privacy with innovation by providing flexible, sector-specific regulations while promoting data localization. POPIA, meanwhile, offers a robust privacy framework in South Africa but remains limited in its enforcement and oversight compared to GDPR.

Each regulatory framework has its unique strengths and challenges in managing AV data, yet all strive to strike a balance between technological advancement and privacy protection. As AV technology evolves, a harmonized approach integrating key elements from these laws—such as GDPR's accountability, DPDPA's adaptability, and POPIA's comprehensive safeguards—could provide an effective global standard. Future policies must remain flexible and adaptive to emerging technologies, ensuring both innovation in autonomous vehicles and the protection of individuals' privacy rights.

REFERENCES

1. B. C. Zanchin, R. Adamshuk, M. M. Santos and K. S. Collazos, "On the instrumentation and classification of autonomous cars," 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Banff, AB, Canada, 2017, pp. 2631-2636, doi: 10.1109/SMC.2017.8123022.

2. Divya, K., and G. Girisha. "Autonomous car data collection and analysis." *Int. Journal of Scientific Research & Engineering Trends* 7.3 (2021)

3.2021 Henry Alexander Ignatious, et al. Published by Elsevier B.V. Abstract reprinted with permission of Elsevier. International Workshop on Smart Communication and Autonomous Driving Ignatious, Henry Alexander ,Sayed, Hesham-El-Khan, Manzoor Publication Date**:** 2022

4. How to hack a self-driving car Ornes, Stephen 2020/08/01 SN - 0953-8585

5. OVER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS Sen Nie, Ling Liu, Yuefeng Du, Wenkai Zhang Keen Security Lab of Tencent

6. Zhang, W., Liu, L., & Nie, S. (2019). "Security Assessment of Connected Cars: A Case Study of BMW." *IEEE Transactions on Intelligent Transportation Systems*.

7.Huang, L., & Wang, Y. (2017). "Adversarial Attacks on Autonomous Driving Systems." *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*