The Human Resource Law on the Personal Data Protection (PDP) in Pakistani Logistic Companies

Erum Naz Akhtar
Manager, Department of Law, Capital University of Science & Technology (CUST), Islamabad

Dr. Tahir Hameed Ullah Khan
Professor/Dean, Department of Law, Capital University of Science & Technology (CUST), Islamabad

Naila rafique
Assistant Professor Law, Capital University of Science & Technology (CUST), Islamabad

Tayyiba Kausar
PhD Scholar, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan

Iram Rehman
PhD Scholar, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan

Ayesha Abbas
PhD Scholar, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan

Corresponding Authour**: **Naila Rafique

Assistant Professor Law, Capital University of Science & Technology (CUST), Islamabad, PK, naila.rafique@cust.edu.pk

Abstract: Nowadays, both government and private entities collect a lot of personal data about people every single day. Personal information is defined as any data about a person that is specific or identifiable. Technology has made it possible for people and organizations to communicate and disseminate knowledge throughout the world. People have every right to have their personal information protected, which guards against unauthorized use by other individuals or organizations. This right is now protected by the amendment to Article 8 of the Constitution of Pakistan. Furthermore, certain additional laws were modified: the current data protection regulations, Pakistan Telecommunications Reorganization Act 1996 (PTA Act), the Electronic Transactions Ordinance 2002 (ETO), the Customs Act 1969, and the

International Journal of Stress Management
2025, Vol. 32, No. 2, 1-19

Prevention of Electronic Crimes Act 2016 (PECA). The legislation imposes strict obligations on all companies that handle, transport, or store personal information. Ordinary and legal individuals are also required to abide by certain rules and procedures. The logistics sector is mainly impacted by the law. This study examines the legal criteria for the security of personal information on a national and international level. The consequences of these restrictions on human resource practices, problems, causes, and impacts in the logistics business have been investigated through a screening process and in-depth interview approaches. Consumers are becoming more conscious of their rights around data privacy. Logistics companies are more likely to win over customers' trust and loyalty if they give them control over their data and are transparent about how they collect, use, and share it. Businesses may gain a competitive edge by implementing robust data protection policies. Consumers are more inclined to choose companies they think would handle their data in an ethical manner. It is expected that this study will contribute to the body of knowledge in the subject and the literature, as there hasn't been much research on this topic.

Keywords: Logistic companies, Human Resource (HR), Personal Data Protection (PDP), Laws and Regulations.

INTRODUCTION

The logistics sector is widely acknowledged to be important, and it is growing both locally and internationally due to the expansion of internet businesses and online shopping patterns. Previously, logistics has been simply referred to as transportation; however, it has developed into a multifaceted industry that includes fundamental phases like production, storage, shipping, packaging, and business growth processes in addition to information technology and customer service. Developments in this area have affected the workforce in the logistics sector. It has contributed to innovations, company expansion, and the competitive environment. The sector depends heavily on human resources and technology. There are numerous companies in Pakistan's logistics sector. Additionally, a significant number of individuals are hired by subsectors. Due to the operational nature of logistics activities, there are a lot more field workers than office workers, and the business has a high personnel turnover rate (Jobnak Human Resources, 2010). In the current climate of fierce rivalry and quick development, human resource departments are essential for businesses. Organizing, overseeing, and providing human resources are among the duties that human resources handle. Human resources are particularly important in the labor-intensive logistics sector, which has multiple company divisions and a high

employee turnover rate. Therefore, these departments must have the knowledge and preparedness to adapt to changing technological, social, and legal environments (Gelincik, n.d.).

The human resources department posts job openings, takes applications, and interviews many candidates. Data is shared throughout each application and interview, and it remains on file whether the applicant is hired or not. After an individual starts working, they continue to share data with workplace norms and procedures. In many aspects of our lives, we routinely document personal data. Since unauthorized people could obtain, use, or misuse the data, it is imperative that it be protected. The right to demand data protection has been granted to individuals.

The Constitution, legislation, and international conventions to which we are parties all safeguard this freedom. In this regard, transmitting someone's identifying information without their agreement is forbidden by Section 16 of the Prevention of Electronic Crimes Act (PECA) 2016. Unauthorized copying and transmission of data with malicious purpose is punishable by up to six months in prison, a fine of up to one hundred thousand rupees, or both under Section 4 of the PECA 2016.The duties, practices, and values of natural and legal people that handle, transport, or store personal data are governed by the law. For people and organizations that break the guidelines, severe fines and incarceration are regulated. The human element is crucial in logistics organizations, which employ people from a variety of areas, have a high labor turnover rate, and handle a lot of personal data. These companies are also intimately tied to the law.

THE CONCEPT OF PERSONAL DATA, ITS BACKGROUND, AND APPLICABLE LAWS

In order to identify areas where different methods tend to diverge and to match common grounds, the Personal Data Protection (PDP) Bill of 2023 was passed in accordance with the current patchwork of regional and international laws on the protection of personal data. A wide range of economic, political and social activities have been digitalized by rapid technological advancement and increased use of internet services. This has had a profound impact on how people interact with each other, with businesses, the government, and other stakeholders. Due to their developmental vulnerabilities, children who are early adopters of developing technologies are likewise impacted by the perils of the digital world, acting as "canaries in the coal mine for threats to us all." Therefore, additional protection for minors' data is guaranteed by the Data Protection Bill of 2023.

To make sure that the potential coming out of the economy can be effectively utilized building trust online is a crucial task. Personal data is a key component of the global economy's transition to a connected information world,

which propels online cross-border commercial activity and whose movement may have an impact on people, companies, and the government. According to the PDP bill, personal information must only be gathered from people legally, fairly, and voluntarily. It must also be used or disclosed for the purposes for which it was collected or for any other directly related purpose.

Essentially, personal data includes information about a person's name, surname, birth date, and place of birth; information that identifies a person's social, physical, economic, or psychological identity; and information that will allow a person to be identified, such as a person's identity, social security number, and phone number. Additionally, a person's resume, photo, audio, fingerprints, and genetic information are all considered personal data. There is additional protection for certain of your personal information. Sensitive (private) data is the definition of this group (Carey, 2009, p. 81). After going through several phases, the laws governing the protection of personal information have taken on their current form.

Information technology advancements from the latter half of the 20th century to the present have grown increasingly noticeable, impacting not only company operations but also every aspect of daily life. These advancements are also having a significant impact on the logistics industry. The legal sector now needs new legislation as a result of rapid digitization. Determining the legal requirements that data processing operations must adhere to has become essential due to the rapid digitization of information and the need to restore the imbalance against the individual. In this way, digitalization and the law pertaining to the protection of personal data are closely intertwined.

In fact, the first laws protecting personal information were passed during the period when computers and databases started processing personal data on a massive scale. Currently, there are laws governing this area in more than 120 states. The rules governing the protection of personal data are based on international conventions, constitutions, and statutes. Additionally, the legislation contains secondary rules, such as bylaws, regulations, and messages published to illustrate how laws are applied.

REGULATIONS WORLDWIDE

An overview of relevant laws around the world is provided in Table 1.

1. In 2016, the General Data Protection Guideline of the European Union was released. Despite being a law that has been implemented in EU nations, it also imposes penalties on businesses that operate outside of the EU under specific circumstances. Companies involved in logistics that do business with EU member states should pay attention to the General Data Protection Regulation’s major rule.

2. The United Nations created the International Labor Organization (ILO) as a specialized agency. Internationally, it is striving to advance workers' rights and social justice. Pakistan has ratified 36 conventions, including the eight fundamental conventions, and has been a significant and active member of the ILO since its founding in 1947. Over the years, the ILO's Governing Body has been populated by representatives of the government, employers, and workers' organizations. Recommendations and the Code of Practice on the Protection of Employees' Personal Data were espoused at the 1996 Committee of Experts conference.

Table 1: The History of Personal Data Protection (Kaya & Taştan, 2018)

Formations	Article	Year
United Nations	The Universal Declaration of Human Rights	1948
EU Council	The European Convention on Human Rights	1950
United Nations	International Civil and Political Rights Covenant	1966
Organization for Economic Cooperation and Development (OECD)	OECD Guidelines for Transnational Personal Data Flows and Privacy Protection	1980
EU Council	Council of Europe Convention No. 108, the Convention for the Protection of Individuals with Respect to Automatic Processing of Personal Data	1981
United Nations	Regulation Guidelines for Computerized Personal Data Files	1990
EU Commission	Directive on Data Protection (95/46/EC)	1995
EU Council	Additional Protocol No. 181 to the Resolution for the Safety of Persons concerning Programmed Processing of Personal Data pertaining to transnational data flows and supervisory authorities	2001
EU Commission	Directive on the Electronic Communications Sector's Processing of Personal Data and Privacy Protection (2002/58/EC)	2002
EU	European Union General Data ProtectionRegulation2016/679(GDPR)	2016
EU Council	Protocol to amend Convention No. 108+, the Resolution for the Protection of People, regarding Programmed Processing of Personal Data	2018

3. The principles set forth in the Council of Europe's espoused sanctions on personal data protection will have an impact on a number of areas, including recruitment, medical bills, systematic study and statistics, product or service direct

promotion, social security, insurance policies, law enforcement agency records, online shopping, telephones, and the usage of internet services. It is noted that the recommendations cover the topic of "Employment." These suggestions were taken into account in our nation while the Personal Data Protection (PDP) Bill 2021 was being prepared. It is believed that the legislation pertaining to various sectors will incorporate these ideas. Meanwhile, the Personal Data Protection Board began formulating its decisions on a number of different areas and issues.

LAW AT THE NATIONAL LEVEL

1. Although Pakistan does not yet have data protection laws, they are comparable to those passed in other nations; currently, the Prevention of PECA 2016 accomplishes a similar goal to some degree.
2. A person's right to confidentiality is also sure by Article 14 of the Pakistani Constitution, and any infringement of this right is seen as a flagrant breach of the document. "The dignity of man, and subject to law, the privacy of the home, shall be inviolable," states Article 14.
3. There is no explicit law in Pakistan that governs the dispensation and transmission of private data; hence the regulatory framework pertaining to data privacy and protection has been weak. Instead, the pertinent laws are dispersed among numerous statutes, rules, and regulations.
4. The Islamic Republic of Pakistan's Constitution upholds the right to privacy as a basic freedom. The Constitution's Article 14(1) affirms that "the dignity of man and, subject to law, the privacy of home, shall be inviolable." The right to privacy, as a fundamental constitutional right, is intended to supersede any other contradictory domestic legal rules. Article 8 of the Constitution states that "any law, or any custom or usage having the force of law, in so far as it is inconsistent with the rights conferred [under the Constitution], shall, to the extent of such inconsistency, be void." Additionally, Article 8(5) declares that "rights granted by this Chapter shall not be interrupted unless specifically permitted by the Constitution."
5. The constitution of Pakistan also has a broad exception to the fundamental rights' precedence. Article 8 does not apply to any law that deals with the "proper discharge" of military or police duties. The extent of this exception is alarming considering the Armed Forces' historical prominence, particularly in Pakistan's internal political landscape. This right includes being aware of, having access to, and seeking the correction and deletion of personal information, as well as being informed if its use is consistent with its intended purposes. Only situations permitted by law or with the express consent of the subject may involve the processing of personal data. The law will establish the guidelines and protocols for protecting personal information. Islamic Republic of Pakistan

Constitution, Article 14 recognizes that everyone has the right to have their personal information protected and forms the basis for all other legislation.

6. Pakistan's PDP Bill 2021 seeks to safeguard personal information while upholding people's rights. It is a bill to regulate the gathering, processing, use, and disclosure of personal information as well as to create and include provisions for offenses related to violating people's right to privacy when personal information is collected, obtained, or processed in any way. The scope and goal of the PDP Bill 2021 include the following:

i. Important terminology like "data controller," "data processor," and "processing" are defined in the bill.

ii. According to the bill, consent must be free, informed, explicit, and unambiguous before processing personal data. Withdrawing consent is as simple as giving it.

iii. According to the bill, personal data cannot be transferred outside of Pakistan unless the recipient nation provides comparable protection.

iv. The bill requires that important personal data be processed in Pakistan.

v. According to the bill, data controllers must maintain documentation of all data processing activities, including data categories, purposes, and security protocols.

LITERATURE REVIEW

The safety of personal information is a significant subject that has recently been covered by laws in many nations. There is now more research in the literature as a result. We live in an era of "information" and "technology," when a large number of personal and economic transactions are conducted online. Additionally, this problem transcends all physical boundaries because people and corporations conduct cross-border transactions electronically. For these reasons, electronic information sharing has made it necessary to protect and preserve any personal information that is gathered and used throughout transactions. Therefore, to ensure privacy and data protection, regulations must be in place for the collecting and processing of personal information.

As detailed above, numerous research studies on personal data protection have been conducted; however, to the best knowledge of the Authors there are no studies on the security of personal information in HR applications in the logistics industry. It is believed that this study will add to the field and literature in this way.

METHOD OF RESEARCH

The study has a qualitative methodological emphasis. Using the exploratory and screening methods, data on the topic under investigation has been gathered from a homogeneous group (logistics companies). One of the best ways for social scientists to gather and characterize natural data is through screening studies. Exploration, description, and explanation are all possible uses for screening research. First, administrative structures, sectoral and case resources, statistics, and rulings from the PDP Board were used. Additionally, by examining samples from official sources, knowledge on various uses for logistics companies has been acquired. After all of this data has been evaluated, suggestions have been made.

Detailed discussions were held with human resources representatives of logistics companies operating in Pakistan, including Qwerty Experts, National Logistics Corporation, H.T. Supplies & Services (Pvt) Limited, and DDS Courier Service. We selected these companies because of their excellent services and customer trust. They were asked about the protection of workers' and customers' personal information and their dedication to data security and privacy. Furthermore, we discussed their expertise with safe data management procedures and asked about examples of how they have protected private data. They explained the distinction between data anonymization and data pseudonymization in their logistics company. They also explained that they abide by the regulatory requirements and corporate standards, which shows their dedication to privacy and data protection. Additionally, we conversed about how they manage sensitive data at work, including the use of encoded communication channels, the storage of paper copies in secured cabinets, and the destruction of documents that must be taken out of storage.

Qwerty Experts provides custom coding, website optimization, and web development services, including performance improvements and Shopify theme customization. Clients appreciate their prompt delivery, lucid communication, and extraordinary attention to detail in their assessments, underscoring their capacity to understand business requirements and provide superior, workable solutions. They claimed that protection of the personal data of their stakeholders is their first priority.

One of Pakistan's top corporate entities is the National Logistics Corporation (NLC), offering high-quality, considerate services to both domestic and foreign clients. The development of infrastructure and business facilitation throughout Pakistan is the goal of NLC, with interests ranging from border terminal facilities to multimodal logistics management. The organization has a strong commitment to enhancing sustainable development initiatives and logistical infrastructure throughout Pakistan. Their data protection system is handled by their IT department using a trackable coding system in their packages, trucks, and shipments.

Haider Traders, founded in 1995, was registered as a corporation in January 2018 and is currently operating under the name H.T. Supplies & Services (Pvt) Limited. This company is considered the best staffing and outsourcing corporation in Pakistan. As a trustworthy service provider, they offer a variety of services, such as production manpower, warehouse housing, packing, labeling, loading and unloading, office staff, merchandise, marketing, IT network systems, maintenance, and sales staff, among other things, in accordance with industry standards. Their HR representative explained all details about stakeholders' data protection, which includes coding, legal protection of documents, etc.

DDS Courier Service claims to offer quick, dependable, safe courier services. Their representative told us that they use a coding system for stakeholders' data protection, and the safety of personal data of all their customers and workers is their topmost priority.

APPLICATIONS FOR HUMAN RESOURCES IN LOGISTICS COMPANIES

Since the legislation on PDP applies to both public and private sectors, it is crucial that employers and employees understand, apply, and modify the legislation to fit their operations. The length of time that firms must register in the system is set by law. If the Registry of Data Controllers registration is not completed, the owners of the businesses will be subject to administrative sanctions of the legislative laws. Depending on the specifics of the incident, compensation and criminal cases may potentially be relevant. All personal data listed in the law is covered by the general provisions of the law. Since the study's focus is on protecting personal information in human resources applications in the logistics industry, this section of the report explains how the policy is applied and how the legislation affects enforcement agencies. Interviews with the companies' human resources have been an integral part of this study.

The human resources officers of the logistics firms where the selection was made participated in detailed in-person interviews. Data was gathered regarding the demands, challenges, and legal applications in the industry. Additionally, information and documentation regarding the law's implementation were gathered from the official websites of numerous logistics companies. The corporations interviewed are headquartered in major cities and have been involved in several commercial sectors (automotive, textile, etc.) both domestically and abroad for many years. It is evident from the history of companies and the range of their operations that many people work in both office and field environments. Consequently, the subject is covered by a number of laws and applications. Because the corporations insist on keeping their names private, the identity of the company cannot be revealed. Before the selection, resources on doctrinal applications, legal requirements, personal data protection, and the collected data

were reviewed. After that, the questions were chosen and the companies were interviewed. During the conference, information was obtained about the existing and new questions, as well as the legal procedures and consequences based on the applications.

INFORMATION GATHERING, APPLICATION, CONSENT, AND PERSONAL DATA

The first step in processing personal data is when candidates apply for jobs posted by companies. Candidates are requested to respond to a series of questions on forms that the employer (the company's human resources department) has produced. In addition to the information on the form, candidates must submit (either in person or online) their exam results, tests, diplomas, certificates, health reports, and other documents. Applications like gaining information about the applicant from a third person or organization, administering assessments, and using cameras and tracking devices are some examples of how personal data is processed. This process is completed by hiring the selected, qualified candidates, extending or even terminating work contracts, or keeping the information of the unemployed interviewees. Therefore, the duty to safeguard, accumulate, remove, destroy, and refrain from transferring all personal data gathered by the manager remains in effect even in the event that the contract is ended or the candidate is not chosen. Even so, there can still be circumstances where an employee's personal information could be in danger. Indeed, many organizations can implement applications like tracking how long an employee uses the restroom, tracking how much the employee moves while using a device in his or her working desk, and banning the use of computers and/or special-purpose phones even during breaks (Uncular, 2018).

As stated earlier, applications for the job ads are the initial step in the human resources process with candidates. The companies that were interviewed were mainly questioned regarding the questions that were asked of applicants in their applications to the job postings and the way that the information was obtained (online, in person, etc.). It will take a long time to finish the processes, the companies said, but they have begun a documentation review since the law was passed. They are reviewing profiles and attached papers from job/worker exploration websites as well as those that are secured within the organization. They said that as part of the study, application forms were updated and the questions posed to applicants were changed to comply with the legislation. Additionally, one of the companies claimed to have provided information about the Law on the Protection of Personal Data (LPPD) to employees who had begun working prior to the law's publication, had them sign consent texts on information

documents, and that the application process would proceed in this manner for those employees to be hired.

All of the businesses claimed that they posted general information under the heading "Protection of personal data and privacy policy" on their official websites in compliance with the legislation. Additionally, they said that in order to give candidates the opportunity to read and learn more before submitting an application, they would include a section on the job requests page of the websites that permitted data processing with the information text. As stated in the study's statutory section, data processors are required to get the candidate's informed agreement before storing any personal information they receive. According to the law's mandatory provisions, it is crucial to give candidates accurate information and get their express agreement before collecting their personal data (the law specifies exceptions if any).

As science and technology have advanced, it is now easier and more common to use applications like electronic and biometric access control systems for worker monitoring, phone snooping, email monitoring, internet access tracking, social media account monitoring, GPS vehicle tracking, and workplace behavior observation. Such requests are subject to the guidelines and principles of the data protection law, as stated in Article 3/3 of the International Labor Organization's (ILO) personal data application code (Uncular, 2018).

Many drivers work in the logistics industry's transportation services, and in order to hire them, both drivers and other applicants must provide certain information and supporting documentation. According to the data and documents gathered for the study, many logistics companies' job application forms and advertisements ask about the candidate's marital status, spouse's name, occupation, number of children, disability if any, and whether a lawsuit or police investigation has been filed against them. Questions about family members, health issues that aren't necessary for a job or duty definition, and matters like criminal history and prior convictions should only be asked of candidates if they are relevant to the job or duty definition (Uncular, 2018). The majority of this data is classified as “Personal Data of Special Nature” under Article 6 of the Personal Data Protection Bill 2020 of Pakistan. According to the companies interviewed during the study, they changed their queries and removed them from their job ads and application forms.

APPLICATION AND SHARING OF PERSONAL DATA

Workers in both domestic and foreign industries can be found in the logistics sector. In this regard, it is also feasible to send employees' personal information overseas. This issue is explained in depth in Section 14 of the PDP Bill 2020 of Pakistan, which states that:

- The country receiving the data offers personal data protection that is at least as strong as what is provided in the bill.
- The data is treated in accordance with the bill and the data subject's consent.
- The Federal Government exempts the data from the requirement due to strategic interests or necessity

The bill also states that critical personal data must be processed in a data center or server located in Pakistan. In the article's continuation, exemptions are listed. When asked, the companies said that they provide foreign workers from the countries where they work (local workers) and that they do not exchange worker personal data between countries in their applications. The National Commission for Personal Data Protection (NCPDP) of Pakistan establishes a data protection framework that regulates the collection, processing, use, disclosure, and transmission of personal data.

THE GLOBAL POSITIONING SYSTEM (GPS), BODY SEARCH, WEARABLE TECHNOLOGY, HEALTH INFORMATION, AND APPLICATIONS

Technological advancements have made it feasible to track automobiles using GPS devices to keep an eye on employees. According to the philosophy, the employer must make it apparent to employees that the tracking device is installed in the work vehicle (truck, van, containers, etc.) and that the vehicle's position, movements, and driving are being recorded. The easiest technique to ensure that the driver can immediately see this message is to place it in each car. According to the businesses surveyed, when hiring new drivers, they are required to sign a paper containing information about GPS in their cars. Workers may be searched on the grounds that it is necessary to stop the illicit removal of valuable items from warehouses or the introduction of hazardous materials. According to the idea, workers should be fully, completely, and clearly informed before such searches are conducted. Additionally, CCTV cameras can be used to watch the areas where employees work, as well as their emails and internet searches. According to rulings on the subject, employers are required to notify employees about the application in a clear and concise manner. According to some of the organizations surveyed, when the law was released, human resources determined how these applications should be processed, and their employees filled out and signed documents during the recruiting process and even included them in employment contracts. Some said they had been notified and would amend their rules accordingly to comply with the law.

Wearable technology is being used by employers more and more to track, monitor, and measure work pace as well as breaks for employees' activities both within and outside of the office. Artificial intelligence is used to analyze the data

gathered from sociometric name tags and badges and calculate worker productivity. Voice and conversation recording should be avoided when using these devices. In the logistics industry, these devices are used to guide warehouse workers to their next task. There will be a violation of rights in the processing of personal data if these device applications are misused. Health information is unique personal information. Only the candidate's or worker's suitability for physical and/or mental recruiting will need to be determined based on the findings of the medical examination (Uncular, 2018). Similarly, during the interviews with the companies, some said that this is how the application is made, while others said that the doctor notifies the worker if they are qualified for the position based on the results of the medical examination and sends a copy of the results to the employee's personal file. Employee health can also be tracked with wearable technology. It would be a violation of the worker's rights to carry out such applications in secret without their consent. Finally, the businesses were questioned about whether they get requests from employees or applicants to delete personal information. The businesses claimed that they had not yet encountered such a circumstance and had not received any requests about this topic.

According to the corporations, they held seminars to gather information and establish a roadmap once the law went into effect. One of the businesses said that they were having trouble putting the legislation into practice, that they were unable to comprehend the law, and that the penalties outlined in the law were excessive. Furthermore, they said that infrastructure investment is necessary to implement regulatory procedures and that the Personal Data Protection Authority should issue the pertinent regulations and other regulatory procedures as soon as feasible. They added that there is a lot of application and labor mobility, particularly in the logistics sector, that the adaptation process should be prolonged, that the process of revising both old and new data takes time, and that they require more time and solutions.

EMPLOYER'S OBLIGATIONS AND CONSEQUENCES

Employers (human resources) are required by the LPPD to notify applicants and employees that they are data controllers and to have their express consent. Pakistan still does not have a law specific to data protection, despite several bills being introduced since 2005. Pakistan passed the PECA 2016, which provides for the protection of citizens' identities in addition to protecting people from cybercrimes. The law stipulates that all ID data cannot be transmitted along with processing, saving, and approval of data owners. This means citizens who use data. Citizens' privacy rights are dedicated to the Pakistan Constitution, but their rights have not been converted to law (Pakistan Data Protection- June 22, 2022).

Furthermore, under the PECA 2016 is Pakistan's primary law in the area of data protection and privacy. Section 4 penalizes the unauthorized copying and transmission of data with dishonest intentions. Section 16 prohibits the transmission of a person's identity information without their consent. Section 38 punishes the transfer of personal or sensitive data without the consent of the person concerned. Sections 3, 4, and 14 require permission before processing, storing, or transmitting data.

Other aspects of data protection and privacy in Pakistan include:

- Sensitive personal data may only be processed with the data subject's consent and in certain circumstances, such as for employment or medical purposes.
- Article 14(1) of the Constitution reaffirms the right to privacy as a fundamental right in the Constitution.
- A "data breach" refers to the unauthorized access, collection, use, disclosure, copying, modification, or destruction of personal data.

The government of Pakistan has appointed the Federal Investigation Agency (FIA) to investigate complaints of PECA violations (PECA of 2016). Employers may not disclose an employee's/candidate's personal data to third parties in violation of the LPPD and may not use it for purposes other than processing. These obligations continue to apply after the employee leaves.

The law grants individuals (workers) the following rights, as mentioned in the Application section: the right to know whether personal data has been processed, the right to request information about whether personal data has been processed, the right to know whether personal data has been used for its intended purpose, the right to know which third parties have received personal data within or outside the country, the right to request that personal data be erased or destroyed, etc. It was also decided what sanctions would be implemented in the event of a violation (Belge, 2017).When all of these factors are taken into account, requests for personal data should be appropriate for the intended use and not go beyond it, and there should be a legitimate relationship made between them for the purpose of collection. Before collecting personal information, the employee should be fully informed. Employers are required to safeguard the data. The law punishes people and organizations that violate rights with heavy penalties and jail time. Ensuring adherence to legal procedures and rules is a major responsibility of the PDP Authority.

EMPLOYER REQUIREMENTS (HUMAN RESOURCES)

The misuse of personal information to influence people without their knowledge is not just concerning but also, to start with, extremely dangerous in the current digital era. Individuals' capacity to actively engage in democracy is jeopardized when they are deceived without even realizing it. This is very

disturbing aspect that should concern us all. Furthermore, this problem is fundamental to what it means to live in a free and informed society. The law concerns all public-private sectors, employers, and workers. Likewise, there are numerous rights violations through data sharing, not only by employers but also by workers.

The internet, however, is not the only place where data and information are appropriated. Contact details and residential addresses of customers were purportedly leaked from the database of a reputable courier service in Lahore recently. This information clearly fell under the category of illegal activities like stalking, harassment, threatening, bullying, and so on. Additionally, it has been frequently claimed that drivers of app-based ride-sharing services (like Uber and Careem) have stolen client data and harassed users, particularly women. In order to inform readers about the laws and legal recourse available for protection, this article attempts to draw attention to instances of data appropriation.

The PECA 2016 is the primary piece of legislation pertaining to data protection and cybercrimes in Pakistan. Its main goals are to acknowledge cybercrimes as real crimes and provide victims with legal recourse. Unauthorized access to information is a relatively typical kind of data appropriation, and this was exactly what happened with the information breach from the above-mentioned courier service. Section 3 of the Act addresses this type of unlawful access and stipulates that anyone found guilty of obtaining information for which they are not permitted faces up to three months in prison and/or a fine of up to PKR 50,000. Sections 16(1) and (2) address the appropriation of identification information and stipulate that anyone who obtains, utilizes, or disseminates someone else's identity information without authorization faces a maximum penalty of three years in jail and/or a fine of PKR 5 million. The victim may contact the Pakistan Telecommunication Authority (PTA), which is then required by the same provision to take any suitable action if the material was also sent online after unlawful access was obtained. Therefore, if victims begin utilizing the remedies provided by this section, the appropriation of information by ride-sharing drivers can also be addressed.

According to section 24 of the PECA 2016, cyberstalking is the act of obtaining someone's information via technology and then using it to coerce, harass, threaten, or stalk that individual. Cyberstalking is a federal crime, carrying a maximum sentence of three years in prison and a fine of up to PKR one million. Under this law, any ride-sharing user or client of the courier company who has experienced harassment as a result of their information being leaked may file a claim. However, a common problem in our nation is that young victims frequently feel pressured to make snap decisions due to the psychological strain that an incident causes.

Information duplication and transmission by unauthorized individuals is forbidden by Section 4. This covers not just the dissemination of state and

business data but also the unauthorized dissemination of images, videos, or any other type of data. The maximum penalty for offenders is PKR 100,000 in fines or up to six months in jail. Since these crimes are frequently perpetrated, particularly against women in our culture, having a legal remedy and penalty would aid in the fight against the problems.

This issue is further addressed in Section 21. It declares that anyone who openly displays any kind of sexual behavior, especially through images or recordings, is in violation of the Act and faces up to five years in prison and/or a fine of up to PKR 5 million. This provision also forbids using such content to blackmail someone and profit from it. Inappropriate photos, films, snapshots, and other media are frequently taken from someone, who is then brutally blackmailed and threatened with the content's exposure or display. Such criminals have ultimately received large sums of money from their victims. They are protected against blackmail under this section (Hubaish Farooqui, Oct 2019).

Targeting the real offender of cybercrime in an organization/institute can be challenging because investigative methods may not be sufficient, and the accused may not be found guilty later. Victims may also target the organization’s HR (Human Resources) for data leaks, although not for the actual conduct, but rather for omissions, that is, failing to stop such crimes from happening. Victims may file a lawsuit against the relevant party in any court of law with the necessary jurisdiction in order to assert a violation of any of the aforementioned provisions. The National Response Center for Cyber Crime (NR3C) is another way to report cybercrimes, harassment, and bullying to the Federal Investigation Agency. Among the issues that the FIA handles are acts pertaining to cyberbullying, picture usage, information transmission, etc. Threatening to release information and images (particularly involving nudity or sexual in nature) is frequently reported to the agency, which will subsequently take any necessary and helpful action. Legal knowledge is crucial in today's society, but sadly, people frequently ignore the laws that are in place and give in to pressure. Online scams and other crimes, including harassment and blackmail, have claimed many lives while the public is unaware of the laws that have been put in place. The government creates laws for us, so it seems sensible that we use them to our advantage and hold the executive and lawmakers responsible for their ineffective execution.

CONCLUSION AND RECOMMENDATIONS

Personal information is gathered while the worker is still a candidate because of the unique nature of labor law. Following the hiring process, an employment contract is created, and the employer-personal data relationship remains within the parameters of the employer's organization authority and the employee's reliance. When the employment contract is canceled, the data stays with the employer. For

human resources that handle data, the Law on the Protection of Personal Data is crucial because it specifies all information for a specific person. The PECA 2016 is Pakistan's main data protection law. The PECA guards against illegal access to personal information and safeguards persons' identity data. The study looked at the particulars of labor law and the state of apps for protecting personal data in the logistics industry. Workers' movement is experienced quickly and intensely in this field. Many personal data entries are completed daily, and there are more field workers than office staff.

This work has been done in a variety of sectors and has an international component. Legal regulations include international treaties to which Pakistan is a party in addition to the laws of its own country. For all of these reasons, human resources officers of logistics organizations should take into account international treaties and the legislation on personal data protection. The early completion of legislation harmonization studies is also crucial. The Law on the Protection of Personal Data Basic Legislation (LPPD) should be the primary focus of training for human resources officials. Recruitment procedures, employee and departing employee identification, information technology infrastructure and business processes for data processing, protection, and storage, inventory preparation studies, documentation training, and LPPD notification of all personnel are among the sub-processes of human resources information training. Basic training includes drafting notices and explicit consent texts, updating work contracts and HR forms in accordance with the law, and publishing them online. The worker should be fully aware and conscious of the subject to which they are consenting, and the employer should tell them of this while gaining their consent. One of the most significant laws, this clause serves as the cornerstone for proper data processing. There isn't a single paper on the topic of this research in the literature.

Legal knowledge is crucial in today's society, but sadly, people frequently ignore the laws that are in place and give in to pressure. Online scams and other crimes, including harassment and blackmail, have claimed many lives while the public is unaware of the laws that have been put in place. The government creates laws for us, so it makes sense that we use them to our advantage and hold the executive and lawmakers responsible for their ineffective execution. The main significance of the present study is that it will add value to the literature as well as the industry since it conceptually tackles the protection of personal data, incorporates national and international legal standards, and offers examples from implementations. On the basis of the study presented in this paper, the key recommendations are as follows:

1. Only collect the information that is strictly required for business operations. Steer clear of gathering too much or unrelated data.
2. Clearly define your data retention guidelines and follow them to the letter. When data is no longer required, anonymize or delete it.

3. Put strong encoding technologies into place to safeguard data while it's in motion and at rest.
4. Implement stringent access controls to restrict authorized persons with a need-to-know basis from accessing data.
5. Perform routine security audits to find and fix vulnerabilities.
6. Hold frequent training sessions to educate staff members on the value of protecting sensitive data and best practices for data protection.
7. Clearly explain security standards and procedures to staff members.
8. Stay informed on Pakistan's pertinent data privacy laws and regulations.
9. Engage with legal counsel to guarantee loyalty to data protection regulations.
10. Be transparent with clients on the collection, usage, and sharing of their data.
11. Perform extensive due diligence on external providers who handle employee or customer data.
12. Include provisions pertaining to data protection in agreements with outside vendors.
13. Use Data Loss Prevention (DLP) tools to monitor and prevent unlawful data transfers.
14. Review and update data protection policies and procedures on a regular basis.
15. Last but not least, create feedback channels to get opinions on data protection procedures from staff members and clients.

We believe that by implementing these recommendations, logistics companies in Pakistan can significantly improve the security of employee and customer data, create trust, and comply with legal requirements.

REFERENCES

Belge, A. (2017). Violations and Protection of Workers' Personal Data, in Particular within the Framework of the Law on the Protection of Personal Data. DEU Journal of Law Faculty. C. 19, Special Issue (p. 1025-1051)

Carey, P. (2009). Data Production. In Oxford, Data Protection: A Practical Guide to UK and EU Law (p. 81). Oxford University Press. Constitution of the Republic of Turkey, (1982) (No: 2709, p. art.20).

Doğan, A. (2017, September 4). New address for irregular employment: Logistics warehouses. İstanbul: Evenest Retrieved from https://www.evrensel.net/haber/331329/kuralsiz-calistirilmanin-yeni-adresi-lojistik-depolari

Gelincik, E. (n.d.). Human Resources and Quality Management in the Logistics Sector. Retrieved from International Transport and Logistics Service Producers Association: https://www.utikad.org.tr/SektorelHaber.aspx?DataID=8645&Baslik

Jobnak Human Resources. (2010, December 23). Why are Human Resources Different in the Logistics Sector? Retrieved from https://tr-tr.facebook.com/notes/jobnak-insan-kaynaklari

Kartal, M. (2018). Protection of Personal Data: A Conceptual Assessment of the Turkish Banking Sector. International Journal of Economics and Innovation,4,(1-18)

Kaya, M.B. & Taştan F.G.(2018), Personal Data Protection Law, On İki Levha Press. Law No6698, (2016) Law on the Protection of Personal Data

Personal Data Protection Board, (2018), Unlawful Sharing of Personal Data of Special Nature on Internet and Social Media Channels, Retrieved from https://www.kvkk.gov.tr/3

Personal Data Protection Authority, (2019). Retrieved from https://www.kvkk.gov.tr/5

https://www.legal500.com/developments/thought-leadership/data-privacy-law-in-pakistan-and-its-applicability-to-employment-practices

https://courtingthelaw.com/2019/10/23/commentary/data-protection-awareness-in-pakistan/

Personal Data Protection Board, (2018), Unlawful Sharing of Personal Data Processed in the Job Application Process, Retrieved from https://www.kvkk.gov.tr/1

Personal Data Protection Board, (2018, May 31) Processing of such data outside the authority and purpose of the personnel authorized to access personal data before the data controller, (No:2018/63) Retrieved from https://www.kvkk.gov.tr/2

Personal Data Protection Board, (2018, May 31) Adequate Measures to be taken by Data Controllers in the Processing of Personal Data of Special Nature, (No: 2018/10) Retrieved from https://www.kvkk.gov.tr/4 Turkish Criminal Code (2004).

Uncular, S. (2018). Protection of Workers Personal Data in Business Relationship. In Seçkin. Ankara. (p.186-187/233)