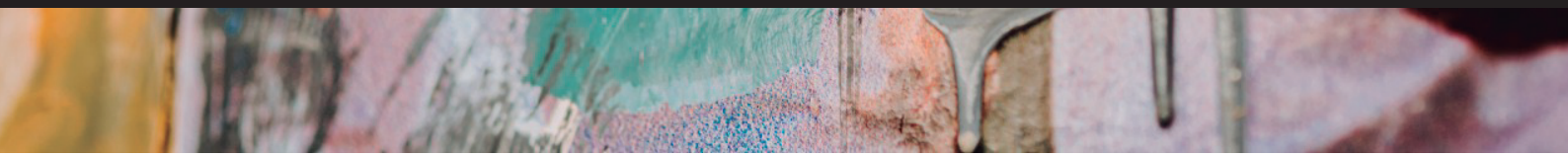


Personal Data Protection and Cybersecurity on the occasion of COVID-19

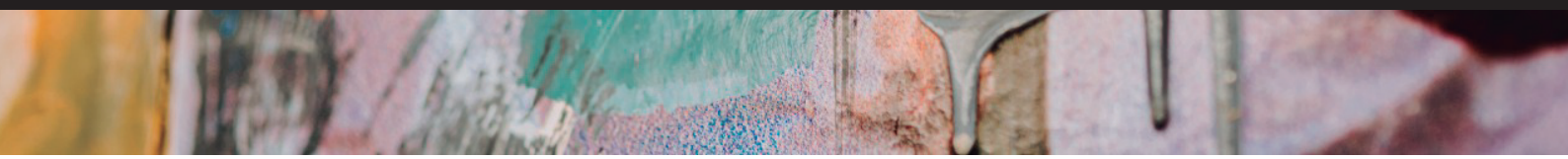
The country-wide Health Emergency and the State of National Emergency declared in Peru at the advent of the international COVID-19 pandemic has faced us with a series of l**egal challenges** to achieve the correct development of the services offered by the public and private sectors; challenges which include the protection of personal data and cyber security.

Many media outlets have revealed images and data of COVID-19 patients without their consent in the midst of the emergency situation, consent which must also be given in writing because such data qualifies as sensitive data. In this regard, the Directorate of Personal Data Protection (the authority in charge, under the Ministry of Justice and Human Rights) has already issued a statement, urging the media not to publish such information. Furthermore, patients' personal data can only be used without consent by the people whose role is the treatment of patients, or for the implementation of public policies to aimed at containing the pandemic. The media may only access and disclose general, unidentified information about the number of patients attended, age, sex, place of infection or other information that does not identify or make patients with COVID-19 identifiable, otherwise they would be committing a **serious infraction, punishable by a fine of up to S/ 215,000.00** (fines for data protection violations range from S/ 2,100 to S/ 420,000).

Also, the authority has recommended to verify that the web pages or applications that perform tests on the COVID-19 and that request data from individuals are reliable pages and that the privacy policies are being read to know the purpose of the use of your information.

Another important aspect to consider is that many companies are implementing remote work solutions (i.e. "home office") through the available technological means, so it is important to be very careful with the information and personal data they handle and protect, as they can be indivertibly misused by unsupervised workers.

Furthermore, services are increasingly being carried out through virtual platforms and web pages, channels through which different information is required from users. Therefore, it is essential that the obligations of the rules on personal data protection are complied with, which are mandatory for all natural or legal persons of public or private law that manage personal data (any information about a natural person that identifies him or her or makes him or her identifiable), even applicable to companies that are not incorporated in the Peruvian territory, but that use means in said territory for the collection of the data.



In Peru, the main rules on personal data protection are

Law 29733, **Law on Personal Data Protection and its Regulations** approved by Supreme Decree No. 003-2013-JUS, regulates the obligations and rights on the subject.

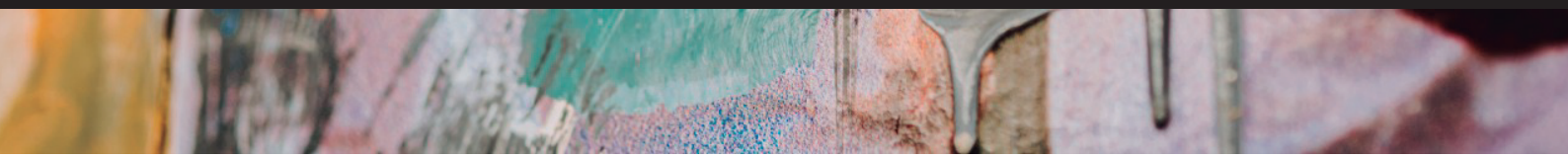
Directive on Security of Information Administered by Personal Data Banks establishes information security criteria, as well as a classification of categories in the processing of personal data (basic, simple, intermediate, complex and critical). Such classification considers criteria such as: the volume of records, number of personal data, period of time for the purpose of the processing, ownership of the data bank, processing of sensitive data, among others.

Practical Guide for the observance of the "Duty to Inform" which aims to guide, in a practical and simple way, people who manage personal databases, on how to comply with the duty/right of information established in the regulations.

Directive on the Processing of Personal Data through Video Surveillance Systems, approved by Directorial Resolution No. 02-2020-JUS, which establishes special provisions and obligations relating to the processing of personal data captured through video surveillance systems or any device that allows the processing of data for security purposes, work control, among others.

From a **criminal perspective**, the protection of personal data is a vital issue, as this information is exposed to computer attacks and to being used for criminal purposes. Cybercrime has intensified in recent weeks as a result of the increased digital interactions during the COVID-19 pandemic. These criminals do not limit their attacks to the geographical location where they are physically located, but extend their actions to any place on the planet; also, cases of cyber-scamming have been identified against citizens, private companies in countries such as the United States, Malaysia, Spain, and even international organizations.

For example, the British news agency Reuters has reported that, during the month of March and in the midst of the spread of the aforementioned virus, the World Health Organization (WHO), the world body that is leading the battle against this disease, has seen a doubling of attempts to hack into the institutional mail accounts of its workers. Likewise, **the BBC has revealed that through the modality of "pishing", the computer hackers have pretended to be the Centers for Disease Control and Prevention of the United States** (CDC) in order to send "emails" with false information about the disease COVID-19 and therefore be able to infect the computers of the recipients, thus obtaining



their personal data, passwords, credit card numbers and other information that could be monetized.

According to TechRadar, another form of computer attack in the form of "malware", working through the false maps or panels that supposedly show updated numbers of people infected by the COVID-19, but in reality, allows hackers to obtain personal information from users who enter and display these maps. With respect to these cases, the U.S. Department of Justice (DOJ) has reported that individuals should seek out reliable sources of information, and especially avoid accessing malicious websites and applications that appear to share disease-related information.

Our country is no stranger to these computer-related tricks and abuse of personal databases. **For example, cyber-criminals can illegally access the database of the National Institute of Statistics and Information (INEI), to manipulate the registered information and improperly obtain the monetary benefit of S/ 380.00 granted by the State to persons in vulnerable conditions. I**f this were to happen, not only would the crime of **computer fraud** (article 8 of Law No. 30096) be aggravated, but it would also produce a sense of distrust among the population itself towards the work of State institutions with regard to the evaluation and selection criteria for the granting of State subsidies.

For all these reasons, it is necessary for government authorities, the private sector and, in general, all Peruvian citizens, to be aware that the cyber-attacks that have occurred in other emerging countries can be replicated in our country, without any major obstacle.

Finally, it is important to point out that in Peru the provisions of the **Law regulating the use of unsolicited commercial e-mail (SPAM)**, Law 28493 and its Regulations, approved by Supreme Decree 031-2005-MTC, regulates the rights of e-mail users: t**he right to refuse or not to receive commercial e-mails, to revoke the authorization to receive them, that their provider has systems or programs that filter unsolicited e-mails**, to forward unsolicited e-mails with a copy to the account implemented by the corresponding authority (INDECOPI). Also, the unsolicited email must comply with the formal characteristics mentioned in the standard and will be considered illegal if it does not meet these characteristics or when it contains false name or false information that is oriented not to identify the natural or legal person transmitting the message, contains false or misleading information in the "subject" field or is sent or transmitted to a recipient who has asked not to receive such advertising. **Failure to comply with the provisions should result in financial compensation to the recipient.**