The State of Communication Privacy Law in Peru

Katitza Rodriguez,
International Rights Director
(EFF)

Veridiana Alimonti,
Latin American Senior Policy
Analyst (EFF)

In collaboration with:

Carlos Guerrero
(Hiperderecho)

Authors: Katitza Rodriguez and Veridiana Alimonti
Collaborators: Carlos Guerrero (Hiperderecho)

This report builds on the *State Communications Surveillance and the Protection of Fundamental Rights in Peru* report, published in 2016.

EFF's Associate Director of Research, Gennie Gebhart edited this report. EFF's Engineering and Design Project Manager, Kim Carlson, along with EFF's Art Director, Hugh D' Andrade and EFF's Education & Design Lead, Soraya Okuda designed and formatted this report. EFF's engineers, Syd Young, Artemis Schatzkin, and Will Greenberg developed the revamped version of the Necessary & Proportionate website.

EFF would like to thank Luiza Rehder do Amaral, EFF Tecs-USP Fellow (2019) for her research and contributions to this report.

A publication of the Electronic Frontier Foundation, 2020.

JUNE 2020

INTRODUCTION

This report provides condensed information on the rules for government access to communication data in criminal investigations in Peru. It offers brief and straightforward answers on a set of relevant questions regarding when and under which conditions law enforcement authorities can gain access to users' communications data in criminal investigations as well as an overview of transparency obligations and practices.

This FAQ is intended for non-lawyers who want some general information about the legal framework for government access to data, but is not legal or technical advice.

The legal questions raised by this FAQ can be complex and the legal risks in any case will depend on the particular facts and on legal doctrines not necessarily mentioned here. This FAQ is meant to familiarize you with some of the principles involved, so that you can have a more effective discussion if and when you engage an attorney to help you with your particular circumstance.

DATA PROTECTION OVERVIEW

1. Is there a data protection law?

Yes. Peru adopted a comprehensive data protection law in 2011.[1] It applies to personal data contained in databases held by public and private bodies, whose processing is carried out in the national territory. The law also subjects sensitive data to a special level of protection.

2. Is there a data protection authority?

Yes. Article 32 of the data protection law created the National Authority for the Protection of Personal Data. The entity responsible for exercising such authority is the General Directorate of Transparency, Access to Public Information, and Protection of Personal Data. It depends hierarchically on the Peruvian Vice Ministerial Office of Justice. It is also the body in charge of exercising the National Authority for Transparency and Access to Public Information.[2] The Data Protection Authority must periodically submit a report on its activities to the Minister of Justice, and receives support and technical advice from the National Office of Electronic Government and Information Technology (ONGEI) of the Presidency of the Council of Ministers.[3]

3. Does the data protection law apply to law enforcement activities?

Article 3 of the data protection law provides specific exemptions from the application of the law: when the databases are administered by public entities when their processing is necessary for them to comply with their powers, and for reasons of national defense or public safety.[4] According to Hiperderecho, different laws and regulations use this exception, for example, laws that require the installation of surveillance cameras, those that create a mechanism to obtain and store geolocation data, those that require biometric authentication, etc.[5] Under these exemptions, different public entities may process personal information without the data subject's consent. These exemptions can also prevent data subjects from making use of their ARCO rights, especially when the data is stored for reasons of public security or defense.[6]

[1] Law 29733, Data Protection Law, July 3, 2011, available at https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf (Spanish)
[2] See General Directorate of Transparency, Access to Public Information and Protection of Personal Data, available at https://www.minjus.gob.pe/dgtaipd (Spanish)
[3] See Article 32, Data Protection Law.
[4] Data Protection Law, Article 3, subsection 2, and Regulation, Article 4, available at https://www.minjus.gob.pe/wp-content/uploads/2013/04/LEY-29733.pdf (Spanish)
[5] See Carlos Guerrero, Hiperderecho, Ley de Protección de Datos y seguridad ciudadana, July 15, 2019, available at https://hiperderecho.org/2019/07/ley-de-proteccion-de-datos-y-seguridad-ciudadana/ (Spanish).
[6] *See* Carlos Guerrero, Hiperderecho, Ley de protección de datos y seguridad ciudadana, July 15, 2019, available at https://hiperderecho.org/2019/07/ley-de-proteccion-de-datos-y-seguridad-ciudadana (Spanish).

4. What are the criteria, if any, for the transfer of personal data to third countries under their data protection law?

Article 15 of the data protection law states that the transfer of personal data to third countries can only be carried out if the recipient country maintains adequate levels of protection in accordance with Peruvian data protection law.

Article 11 of the data protection law establishes that Peru must guarantee a sufficient level of protection for the personal data to be processed or, at least, a level comparable to the provisions of the data protection law or international standards in the subject.

COMMUNICATIONS PRIVACY LAW

5. What's the legal authorization needed to access communications data?

Peru's Constitution states that private communications can only be opened, seized, intercepted or intervened by a reasoned judicial order, issued in accordance with legal rules and safeguards.[7] Law 27697,[8] Criminal Code,[9] Criminal Procedure Code,[10] and the protocol of joint action, implemented by Ministerial Order Nº 0243-2014-JUS,[11] regulate the interception of telephone or other forms of communications.

Interception of communication and seizure of digital communications

Article 226 of the Criminal Procedure Code regulates the procedure for the interception of postal communications, such as letters, documents, telegrams, and other kinds of objects sent by mail. It also includes the seizure of stored digital communications or backed up messages.[12] This type of interception can only occur at the prosecutor's request and with judicial authorization issued by the judge in charge of the preliminary investigation. This interception should prove absolutely essential to continuing with the investigation. It may continue until necessary, but it can not continue after the investigation has finished. The judge responsible for the preliminary investigation will decide the legality of the request immediately, through a confidential procedure. The denial of the measure may be appealed by the prosecutor, and it will also be immediately examined by the Superior Court in a confidential manner and without any procedure.[13]

[7] Article 2 (10), Peru's Constitution, (*Constitución Política del Perú*) https://www.minjus.gob.pe/wp-content/uploads/2019/05/Constitucion-Politica-del-Peru-marzo-2019_WEB.pdf (Spanish)
[8] Law 27697, Law that grants the prosecutor to intervene and control communications and private documents in an exceptional Case (Ley que otorga facultad al Fiscal para la intervención y control de comunicaciones y documentos privados en caso excepcional), available at http://www4.congreso.gob.pe/comisiones/2001/justicia/ley27697.htm (Spanish).
[9] Legislative Decree 635, Penal Code, http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf (Spanish).
[10] Criminal Procedural Code http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPROCESALPENAL.pdf (Spanish).
[11] Protocolos relacionados a medida limitativas de allanamiento,impedimento de salida, intervención o grabación de registro de comunicaciones telefónicas o de otras formas de comunicación y levantamiento del secreto bancario, reserva tributaria y bursátil, https://busquedas.elperuano.pe/normaslegales/aprueban-protocolos-de-actuacion-conjunta-relacionados-a-m-rm-n-0243-2014-jus-1163406-1 (Spanish)
[12] Legislative Decree 635, Penal Code, Article 226 (3) http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPROCESALPENAL.pdf (Spanish)
[13] Criminal Procedural Code http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPROCESALPENAL.pdf (Spanish).

Intervention of communications, including access to metadata and location data

Article 230 of the Criminal Procedure Code indicates that whenever there exists sufficient evidence to consider the commission of a crime punishable by over four years in prison, the prosecutor may request the judge in charge of the preliminary investigation to intervene and record telephone, radio, or other kinds of communications. The court order may be directed against the person under investigation or against persons who may be assumed to be connected with the person under investigation, or that the person under investigation uses these other person's communication.

The request and the judicial decision authorizing the intervention should indicate the name and address of the affected person, as well as the identification of the telephone or any other type of telecommunications being intervened, recorded, or registered. They should also describe the form of interception, its scope and duration, and the police unit and prosecutors conducting the intervention, recording, or registering actions.

Telecom service providers must immediately provide cell phone location data, wiretapping, or recording of communications that have been ordered by a court in real time and continuously, upon threat of liability in case of non-compliance. The companies' employees must maintain confidentiality about the request unless they are summoned as a witness to the procedure. If the evidence used to order the measure disappears or a duration of 60 days has elapsed, interception must be stopped immediately. In exceptional cases, the order may be extended upon prior request from the prosecutor and a reasoned decision by the Judge of the Preparatory Investigation.

Article 231 of the Criminal Procedure Code establishes that communications must be registered by recording in order to guarantee accuracy. In addition, it stipulates that all recordings, signs, or evidence collected during the procedure ordered by the judge, as well as the Protocol of Collection and Monitoring, shall be delivered to the prosecutor, who is in charge of preserving them and ensuring their confidentiality.

6. What's the factual basis to access communications data?

The intervention of communication includes two processes: collection and control. The first part is the collection or recording of the conversation and/or its medium, and can be done in a specific communication or in a set of indeterminate ones, within which it should be probable, for reasons that must be duly justified in the request, that it will be useful for the investigation. The second part is the control or knowledge of the communications or parts of it, where those parts that are irrelevant for the purposes of the investigation should be discarded.[14]

[14] Article 2 of Law 27697, available at http://www4.congreso.gob.pe/comisiones/2001/justicia/ley27697.htm (Spanish)

Article 1 of Law 27697 legislates on the constitutional power given to the judges regarding the intervention communications in exceptional cases. It states that it can only be carried out in the following crimes: kidnapping, human trafficking, child pornography, aggravated robbery, extortion, drug trafficking, migrant smuggling, crimes against humanity, crimes against national security and treason against the nation, embezzlement, corruption of public officials, terrorism, tax and customs crimes, money laundering, and cyber crime.[15]

The Criminal Procedure Code sets out that the request that the prosecutor sends to the judge must be reasoned and contain all the necessary data.[16] It must include evidence that allows the judge to grant, under his or her judgment, the corresponding authorization. If the request is denied, the prosecutor may appeal the judgment to a hierarchical superior starting the day after he or she is notified. The prosecutor's request and the judicial authorization must contain the necessary specifications to distinguish the different types of collection and monitoring that are intended to be conducted, including: if a certain communication is going to take place either in an indeterminate group of communications, or under particular circumstances; if the communication is going to take place in the future or has already taken place; if the communication is closed or encrypted; if the communication's sender, recipient, or any other individual connected to the communication has tried to hide either their identity or any fact or circumstance mentioned in the communication; and if access to or the identification of the communication or any of its parts, or the information transmitted, has been obstructed in any way.[17]

During the authorized time span for collection, the prosecutor may regularly monitor the data collected so far, provided that the collecting method is compatible with this practice. If any other evidence of criminal acts is discovered during this period, the prosecutor should notify the competent judge for him or her to decide whether the acts are relevant to the current investigation, or for the Public Prosecutor's Office to determine whether the discovered acts require criminal investigation.

Law 27697 establishes that those involved in the process of investigation—the judge, court staff, the prosecutor, the prosecutor's support team, the Peruvian National Police, judicial experts, attorney generals, and any natural or legal authorized persons—should maintain confidentiality of the information obtained during the investigation. Violation of confidentiality is penalized with disqualification regardless of the applicable criminal, civil, and administrative consequences.

[15] Article 2 of Law 27697.
[16] Article 230 Criminal Procedure Code.
[17] Article 2, of Law 27697.

7. Which authorities have the legal capacity to request access to communications data?

Intervention of communications can only be requested by criminal prosecutors, attorneys general, and the national prosecutor.[18] Interception of communications is conducted by the Public Prosecutor's Office-authorized personnel and/or the Peruvian National Police under the supervision of the prosecutor in charge of the investigation. The law outlines that communications companies should provide them with the technical support needed in order to guarantee the interception and wiretapping of communications. They may also request the support of natural or legal persons experts in information collection activities. Access to cell phone or electronic device location data in *flagrante delicto* cases can be requested by the Peruvian National Police without a warrant.

8. Does the country have provisions about access to data in cases of emergency?

Location tracking in *flagrante delicto* cases

Legislative Decree 1182 grants the specialized police investigation unit the power to request from telecom operators access to real-time cell phone or electronic device location data without a warrant, and when the following three requirements are met simultaneously: when there is a blatant crime (*delito flagrante*, in Spanish),[19] when the punishment for the crime under investigation is greater than four years of imprisonment, and when access to this information is necessary to the investigation. Judicial assessment of the said requirements is carried out after the police have already accessed the data. To that purpose, the unit responsible for the police investigation must send the prosecutor a report justifying its access request within twenty-four hours. Then, the prosecutor will have 24 additional hours to request the "validation of the measure" to a judge. The judge, after receiving the request, has an additional 24 hours to take a stance on the legality of the request and to set a period during which it shall be in force. This means that up to 72 hours may go by from the time the police start to access real-time location data until the time the judge verifies the request and its legality and assesses if all the requirements have been met.

Legislative Decree 1182 also sets out a liability regime for police agents who use this system maliciously,[20] and establishes that the operators must keep confidentiality of the information given to the police under this mechanism. In 2015, Peruvian news reported that the Ministry of the Interior signed with Internet service providers such as Telefónica del Perú, Claro, Bitel, and Entel a secret protocol for police access to location

[18] Article 226 from the Criminal Procedure Code.
[19] "Delito flagrante," in Spanish. A flagrant crime is a crime that has just been committed, is being committed, or was committed in the past 24 hours, Article 259 Criminal Procedural Code.
[20] Legislative Decree 1182, Article 7, available at https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-que-regula-el-uso-de-los-datos-derivados-decreto-legislativo-n-1182-1268121-1/ (Spanish).

data to implement the Legislative Decree 1182.[21] As of 2020, the document remains classified.[22]

Interception in emergency cases

The Criminal Procedure Code allows for an emergency mechanism applicable exclusively when there is an acknowledgment of new subjects or telephone numbers requiring interception in order to prevent imminent terrorism, drug trafficking, or kidnapping offenses. Under these circumstances, the interception may only be ordered by the prosecutor, as long as they subsequently notify the judge for the revision of such measure.[23] In investigations related to violent or serious crimes or criminal organizations, the prosecutor, on their own initiative or upon police request, may conduct surveillance activities through photographs and any other special technical means of observation without notifying the affected person. The need for judicial authorization applies only when said activities are performed indoors.[24]

Special procedure on information collection in case of emergency

Legislative Decree 1141 further establishes that, in cases of national security and under emergency situations, the Director of National Intelligence may, exceptionally, authorize the execution of a special procedure of information collection, and should immediately legalize the request before the ad hoc superior judge. The judge may, within the following 24 hours, ratify or deny it. In the case of a denial, an appeal follows.[25]

9. Is there any data retention mandate?

Legislative Decree 1182 compels telecom companies to keep metadata for 12 months and disclose the data upon judicial authorization in real time. After 12 months, telecom companies are still required to retain such data for an additional 24 months, but can hand over it within seven days upon judicial authorization.[26]

Before Legislative Decree 1182, the only existing obligation on companies was to keep information that was likely to be supervised by the regulatory authority and the information of call records for up to two months. However, under this legislative decree,

[21] Policía considera “reservada” la forma en la que aplica la #LeyStalker (Police considered "reserved" the way in which the #LeyStalker applies, available at https://hiperderecho.org/2016/02/policia-ley-stalker-reservada-la-forma-en-la-que-aplica-la-leystalker (Spanish)
[22] Hiperderecho, Vigilancia Estatal y Transparencia en Perú, available at https://hiperderecho.org/2017/09/vigilancia-estatal-transparencia-peru (Spanish)
[23] Article 231 from Criminal Procedure Code.
[24] Article 207 from Criminal Procedure Code.
[25] Protocolos de Actuación Conjunta" relacionados a medida limitativas de allanamiento,impedimento de salida, intervención o grabación de registro de comunicaciones telefónicas o de otras formas de comunicación y levantamiento del secreto bancario, reserva tributaria y bursátil. https://busquedas.elperuano.pe/normaslegales/decreto-legislativo-de-fortalecimiento-y-modernizacion-del-s-decreto-legislativo-n-1141-876803-2 (Spanish)
[26] Decreto Legislativo 1182, available at https://www.accessnow.org/cms/assets/uploads/archive/Peru_Data_Retention.pdf (Spanish)

these regulations have not been repealed. On one hand, Law 27336 stipulates that all entities under the supervision of the Supervisory Body for Private Investment in Telecommunications (OSIPTEL, by its Spanish acronym) have the obligation to keep, for at least three years, information like valuation, details of call records, invoices, and any information that must be kept in order to comply with the technical standards mandated by a competent authority, or with contractual or statutory obligations applicable to these services.[27] On the other hand, the regulation on users' rights passed by OSIPTEL—the Terms of Use of Public Telecommunications Services—stipulates a similar obligation to keep records. However, this one is much narrower.[28] Specifically, Article 65 of the Terms of Use lays out that the subscribers have the right to request a copy of their incoming calls records from the past 2 months from the operating companies. Accordingly, the operating companies are compelled to keep the information of subscribers' incoming and outgoing calls for at least 2 months to comply with this obligation.

10. Are there any rules that authorize the use of malware?

There are currently no laws that explicitly authorize the use of malware.

11. Is there any law that compels companies to provide direct access to their internal servers for law enforcement purposes?

Article 230 of the Criminal Procedure Code establishes that telecom service providers must provide, immediately, cell phone location data, wiretapping, or recording of communications that have been ordered by a court in real time and continuously, upon threat of liability in case of non-compliance. It further compels telecom providers to enable access, compatibility, and connection between the telecom companies' technology and the Peruvian National Police System of Interception and Monitoring of Communications. It further establishes that whenever the telecom company renews their equipment and software, they are compelled to maintain compatibility with the Peruvian National Police System of Interception and Monitoring of Communications.

[27] Article 16, e from Law 27336, Law on the development of the functions and powers of the Supervisory Body for Private Investment in Telecommunications - OSIPTEL (*Ley de desarrollo de las funciones y facultades del organismo supervisor de inversión privada en telecomunicaciones - OSIPTEL*), available at http://transparencia.mtc.gob.pe/idm_docs/normas_legales/1_0_126.pdf (Spanish)
[28] *Board of Directive Resolution Nº 138-2012-cd-OSIPTEL* https://www.osiptel.gob.pe/repositorioaps/data/1/1/1/par/res1382012cd/Resolucion138-2012-CD-OSIPTEL_TUO-Condiciones-Uso-Servicios-Publicos-Telecomunicaciones3.pdf (Spanish)

12. Does the law compel companies to assist law enforcement agencies in their investigations?

Legislative Decree 1182 makes telecom companies liable if they fail to comply with the data retention obligations established by the Decree. Similar obligations on companies are detailed in article 230 of the Criminal Procedure Code described above (see question 11).

TRANSPARENCY & COMMUNICATIONS PRIVACY

13. Does the State report on the number of requests to access communications data?

The Law of Transparency and Access to Public Information compels the State to make public the information that it creates or that is in its possession, with certain exceptions. The State should be able to make available statistical information about numbers of governments requests to access communications data in criminal investigations if the information has not been classified as secret, reserved, or confidential and if it does not reveal personal data. However, in practice, the information on the details of the requests (quantity, percentage of acceptance or rejection, cases resolved, cases pending resolution, closed cases, etc.) can only be accessed through FOIA requests if that report has already been produced. In exceptional cases, the Transparency Law can declare certain information reserved and not to be delivered when the information impedes the course of the police investigations: for example, reward systems, witness protection, or the interception of communications itself.[29]

14. Is there any legal limitation that prohibits companies from publishing transparency reports?

To the best of our knowledge, no normative framework prohibits companies from publishing statistical data on the number of data requests made by the State in criminal or national security matters. That said, the Transparency Law does prohibit the publication of protocols that have been labeled as secret such as the protocol to access geolocation in real time by the Police, currently in force.

15. Do telecommunication companies publish transparency reports?

- Telefónica-Movistar publishes yearly transparency reports.
- Claro has not published any transparency reports.
- Entel has not published any transparency reports.
- Olo has not published any transparency reports.

[29] Article 16 from Law 27806, Single Ordered Text of Law 27806, Transparency Law and Access to public information, available at https://sistemas06.minedu.gob.pe/sisolai/docs/ley-27806.pdf (Spanish).

- Bitel has not published any transparency reports.
- Inkacel has not published any transparency reports.

16. Can companies notify users about States' data requests?

The Criminal Procedure Code states that once a judicial intervention measure has been carried out and immediate investigations have been carried out considering the result, the affected party must be informed of the measure whenever the investigation scope allows it and as long as it does not endanger the life or bodily integrity of third parties. When the investigation has finished, the individual being surveilled must be notified about the procedures conducted.[30] The individual may ask for judicial re-examination within three days of receiving notice. In said hearing, the judge shall determine the appropriateness of the procedure and the relation of the intercepted and seized communications to the investigation.

Regarding Legislative Decree 1182, there is no obligation to notify users, but such notification could be executed by the companies if it does not contravene the law, in the same terms of judicial interventions explained before. However there is no public information available to verify if this practice is being implemented or even considered as a possibility.

[30] Article 227 from Criminal Procedure Code.