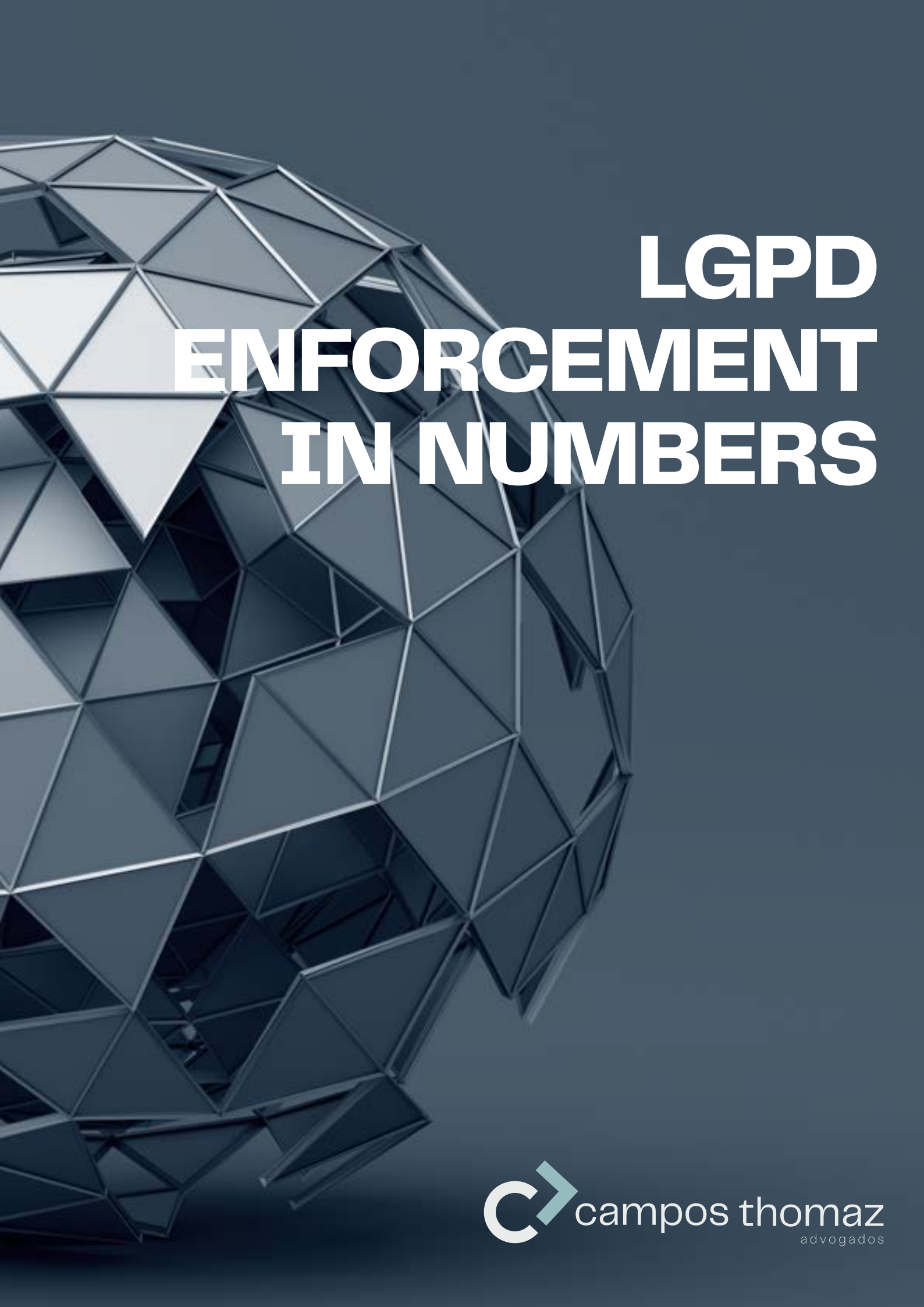


LGPD ENFORCEMENT IN NUMBERS

campos thomaz
advogados

The Brazilian General Data Protection Law (LGPD) completes 5 years in 2023, presenting advances and challenges in its implementation. Published on August 14th, 2018, it only became effective in September 2020 and its planned sanctions started to be valid only in August 2021, being, therefore, a law of recent application. Given its importance, it is increasingly cited and present in the decisions of the Judiciary. From an analysis of the decisions and understandings of the main courts of the country it is possible to identify certain trends and perspectives on the norm.

The following conclusions were drawn from a sample of 438 decisions in the period from 01/01/2022 to 12/31/2022, published in second instance and in higher courts (STJ) by the following courts:

- Superior Court of Justice (STJ)
- Court of Appeals of Bahia (TJBA)
- Court of Appeals of Goiás (TJGO)
- Court of Appeals of Santa Catarina (TJSC)
- Court of Appeals of São Paulo (TJSP)
- Court of Appeals of the Federal District and Territories (TJDFT)
- Court of Appeals of Paraná (TJPR)
- Court of Appeals of Rio de Janeiro (TJRJ)

How decisions involving the LGPD are assigned by the courts

There is a clear predominance for the Court of Appeals of the State of São Paulo (TJSP) to deliver decisions related to the LGPD, which is responsible for 84% of the decisions analyzed. This preponderance in relation to the other courts – which account for only 16% of the decisions – is mainly explained by technical reasons relating to the system used by each Court, in addition to their ability to provide data structured by such systems. See the proportion:

TJSP	84%	TJDFT	2%
TJBA	3%	STJ	1%
TJRJ	2%	TJGO	1%
TJPR	2%	TJSC	5%

— Main findings and trends

1. The majority of legal proceedings related to the LGPD did not result in adverse judgment

Approximately 57% of the decisions analyzed in second or higher instance that dealt with the matter did not result in any adverse judgment (the case was dismissed or extinguished).

2. Decisions in second or higher instance that involve the LGPD tend not to generate obligations to do or not to do

In 41% of the cases, adverse judgments only resulted in monetary compensation (without obligations to do or not to do). In 20% of the cases, it was observed that adverse judgments only referred to obligations to do or not to do (there was no monetary compensation). And in 39% of the decisions rendered, there was an adverse judgment in obligation to do or not to do and monetary compensation (at the same time).

3. Regarding the subject of debt collection and credit protection, it was found that sharing personal data with third parties for this purpose does not require the consent of the data subject

Sharing personal data with third parties, specifically for the purpose of debt collection or credit protection, is generally considered legitimate by judges, regardless of consent. In 53% of the cases, there was an express understanding that consent is not required for this situation. Additionally, when the same sharing is not considered legitimate, it occurs for reasons other than the absence of the data subject's consent, which is considered in rare circumstances, totaling only 6% of the cases.

4. The occurrence of personal data misuse has a higher risk when there is no proper transparency towards the data subject

It was found that 82% of the situations where personal data was processed for an inappropriate purpose generated some type of condemnation. However, in cases where decisions also dealt with the lack of proper transparency in processing, the number is even higher, totaling 91% of the cases.

5. Personal data incidents are not the main motivation for actions that reach the second instance

45% of the decisions in the second or higher instance that deal with the LGPD were motivated by situations involving debt collection or credit protection.

6. In most cases, it was necessary to prove moral damages in order to obtain an adverse judgment

The proof of moral damages was observed in 65% of the analyzed decisions, which in itself indicates a tendency that it does not have an in re ipsa (presumed) nature. In cases of moral damages caused by incidents, the requirement for proof was even higher, occurring in 80% of the cases. However, if caused by sharing or disclosure of personal data, the number drops to 45%, meaning that proof is waived in most of these cases.

7. The right to deletion is the most demanded

Regarding the rights of data subjects (Art. 18), it was found that the right to deletion (items IV and VI of the LGPD) was the most demanded, cited in 64% of the decisions, with an adverse judgment rate of 97%.[1]

— Adverse judgments

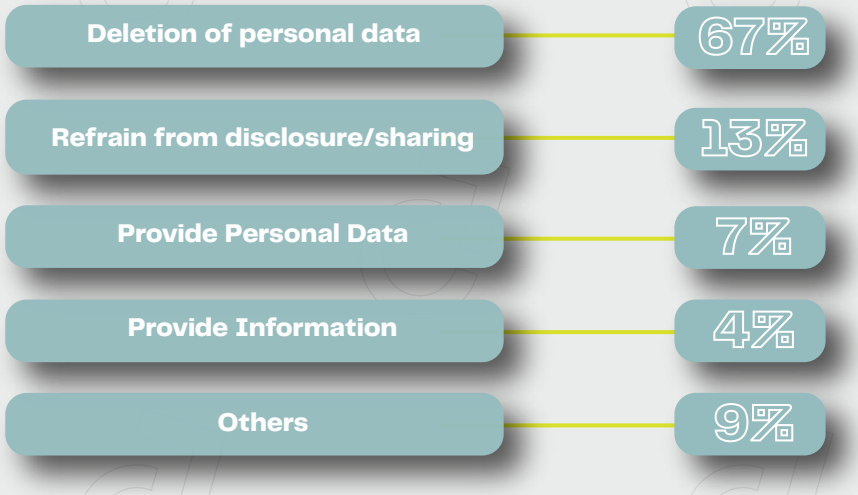
Among the considered decisions, some patterns of results regarding the frequency of adverse judgments were extracted. Basically, it was revealed that 57% of the decisions did not result in adverse judgment or maintenance of adverse judgment, while 43% did.

In addition, the predominance of awards (e.g., compensation) compared to obligations to do or not to do (e.g., elimination by the defendant of such personal data) is notable, representing 80% of the analyzed decisions, which leads to the conclusion of a greater tendency to file actions in court in cases where there is an actual damage to be compensated due to possible illicit facts in the processing of personal data, encompassing both pecuniary and moral damages.

However, obligations to do or not to do totaled 59% of the considered decisions, which highlights the protection of the rights of data subjects, exercised by the contentious jurisdiction, regardless of the need for compensation for possible illegalities related to the processing of personal data.

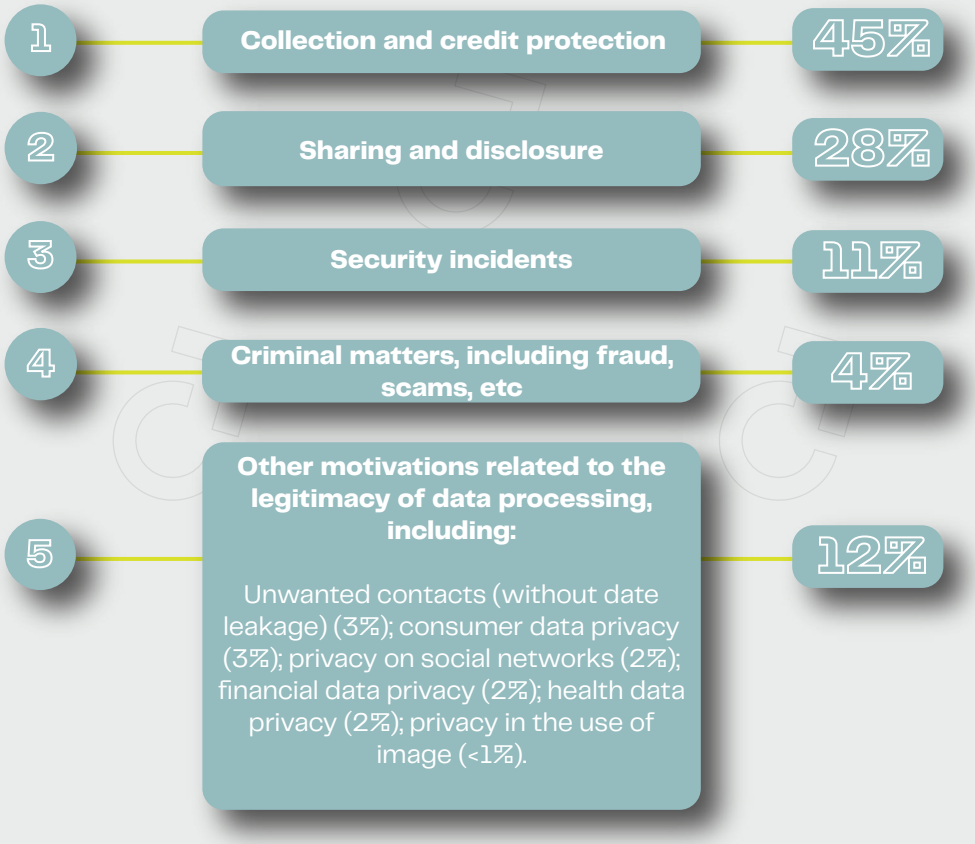
It is also noteworthy that in 39% of the decisions, there was an adverse judgment in obligations to do or not to do cumulatively with an award, indicating the intention of the Judiciary to remedy and repair violations of the rights of data subjects.

— Main obligations to do found



— Motivations

Different motivations were identified in the analyzed decisions. The five most recurrent motivations related to data processing issues were, respectively:



1. COLLECTIONS AND CREDIT PROTECTION

This is a very frequent motivation, present in 45% of the evaluated cases. The considerable predominance of this theme in relation to other motivations (55%) reveals the potential use, by plaintiffs, of the Informed Self-Determination, a principle of the LGPD that characterizes the right to understand and express a positioning on the flow of their data, from the moment they are captured until their disposal.

Regarding the amount of adverse judgments that involve collections and credit protection, they vary according to the nature of the compensation:

Moral damages	From BRL 3,000.00 to BRL 15,000.00
Pecuniary damages	From BRL 1,406.88 to BRL 10,000.00

The need for the data subject's consent for the sharing of their personal data for the purposes of credit protection or collection

It was observed that in decisions dealing with collections and credit protection in which the judge determined the illegitimacy of sharing, consent for sharing was generally not required, being required in only 6% of the cases.

Requirement for consent in cases of illegitimate sharing:

Consent was required	6%
Consent was not required	94%

When legitimacy of sharing was determined, consent was waived in 53% of the cases.

Requirement for consent in cases of legitimate sharing:

Consent was waived	53%
Consent was not waived	47%

Thus, it is possible to conclude that the Judiciary does not require consent for the sharing of personal data for credit and collection purposes. The legitimacy of the sharing of personal data does not depend on the consent of the data subject.

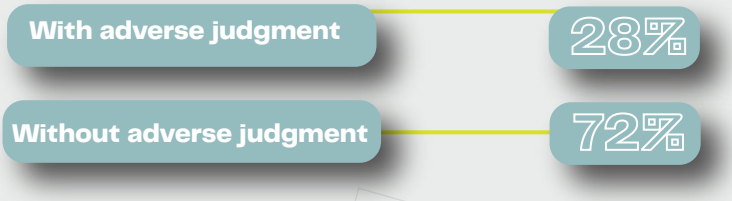
2. SHARING AND DISCLOSURE OF PERSONAL DATA

A significant number of decisions from the second or higher instance were found, in which the plaintiff alleges the sharing and unauthorized disclosure of their personal data, totaling 28% of the cases.

Frequency of Sharing/Disclosure:

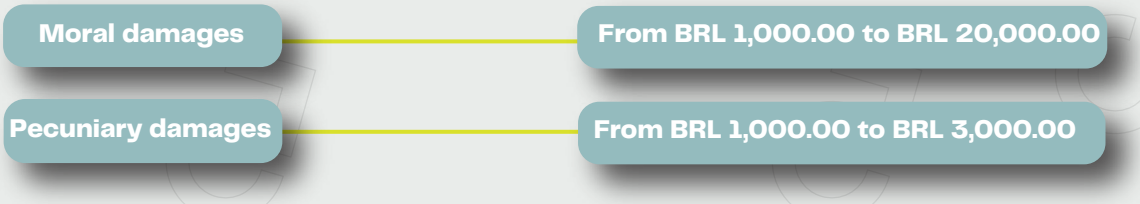
Next, the frequency of adverse judgments regarding the subject was observed, which coincidentally also occurred in 28% of the analyzed cases.

Frequency of Adverse judgments:



Regarding the amounts of adverse judgments involving the sharing and/or unauthorized disclosure of personal data, on average, they are higher when granted as moral damages and lower with regard to pecuniary damages.

Sharing and Disclosure – Adverse judgments:



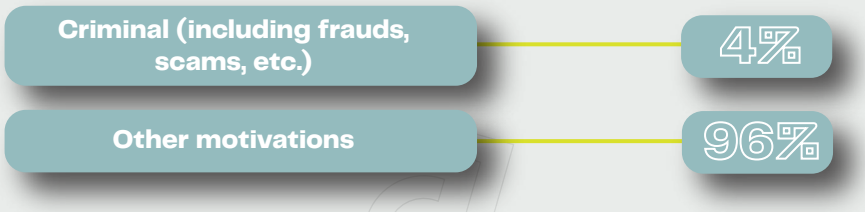
3. DATA BREACH INCIDENT

It was identified that approximately 11% of the motivations in the analyzed cases alleged a data breach incident. However, this allegation occurs more frequently as an ancillary allegation in other actions of different motivations, probably due to the interpretation made by the General Data Protection Law (LGPD) in the sense that inadequate or unlawful processing, mainly with the potential to cause harm to data subjects, can be considered incidents.

4. CASES RELATED TO POTENTIALLY CRIMINAL MATTERS

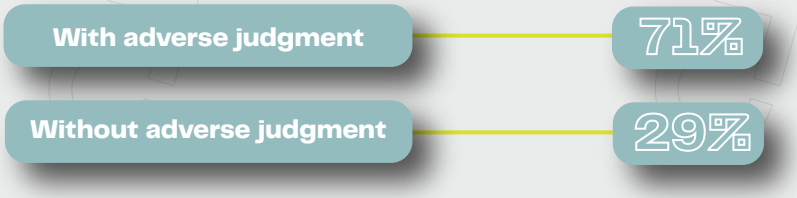
When considering the specificities of the cases, it was often observed that there were potentially criminal matters related to other themes, such as the improper sharing and/or disclosure of personal data. Thus, the sample of these cases is quite comprehensive, considering not only decisions in the criminal sphere, but also in the civil sphere, as long as they are related to potentially criminal facts, including frauds and scams.

Criminal – Frequency of Occurrences:



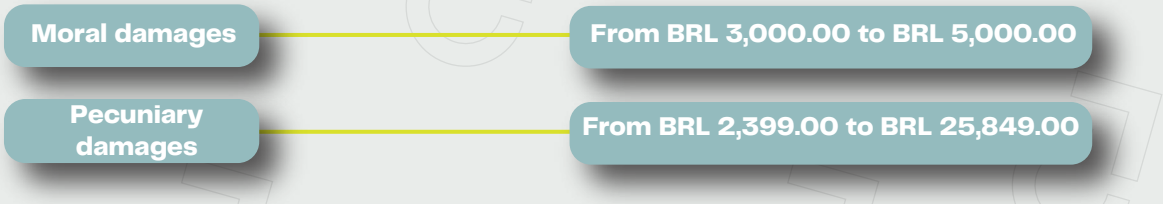
When observing the frequency of occurrences related to the situations mentioned above, it is around 4% of the cases.
Adverse judgments occurred in 71% of the analyzed cases.

Frequency of Adverse judgments:



Regarding compensation values, a greater range was observed for pecuniary damages.

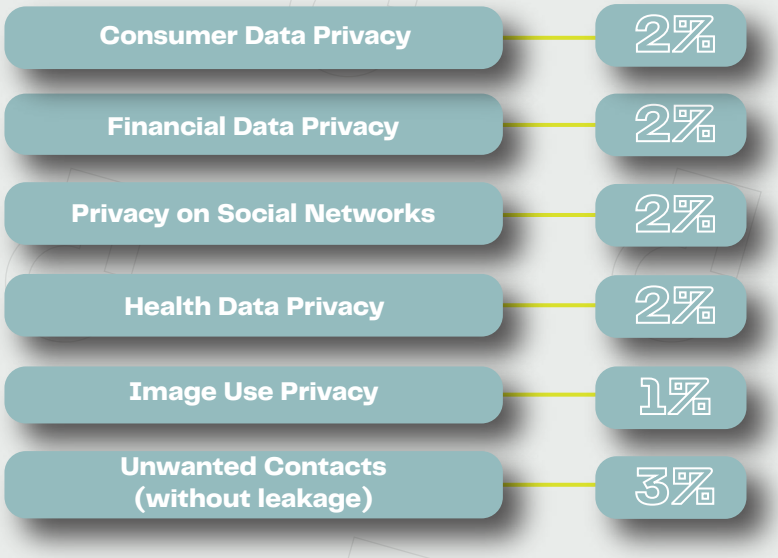
Minimum and maximum compensation values:



5. OTHER MOTIVATIONS RELATED TO THE LEGITIMACY OF PERSONAL DATA PROCESSING

A series of other motivations involving the legitimacy of personal data processing was also identified, however, it represents a minority of the cases.

These other identified motivations include:

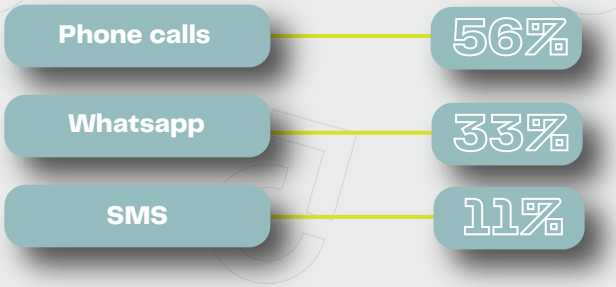


Among these motivations, it is worth noting that unwanted contacts and issues related to the processing of consumer data in a generic way are the most recurrent.

Regarding the value of the adverse judgments, the few that occurred and determined compensation for moral damages in these cases ranged from BRL 500.00 to BRL 9,500.00. There were no substantial numbers regarding compensation for pecuniary damages adverse judgment.

Finally, it should be highlighted that most cases of unwanted contacts involve phone calls, accounting for 56% of the cases.

Types of Unwanted Contacts:



6. RELEVANT THEMES

In addition to the motivations already discussed, other themes relevant to the study in question were mentioned. Considering a sample of 117 decisions, the following was found:

- a) Lack of transparency 92 occurrences
- b) Misuse of data 61 ocurrences
- c) Data subject's rights 45 ocurrences
- d) Security/Breach 21 ocurrences

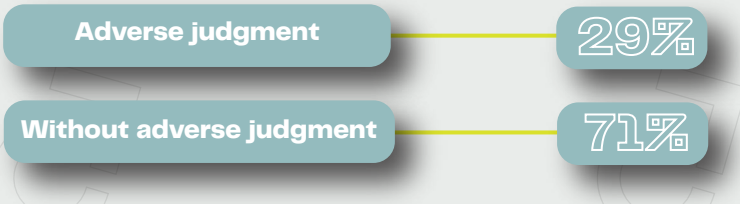
We will analyze each topic separately below:

A. Security/Breach

The mentions related to security/breach incidents encompass decisions that recognize that a "security breach" has caused unauthorized access, alteration, loss, or exposure of personal data.

Frequency

It was found that approximately 12% of all analyzed decisions dealt with discussions involving security incidents. Regarding the frequency of adverse judgments, it was observed that 29% of the cases covered by the current research resulted in adverse judgments.



Compensation values

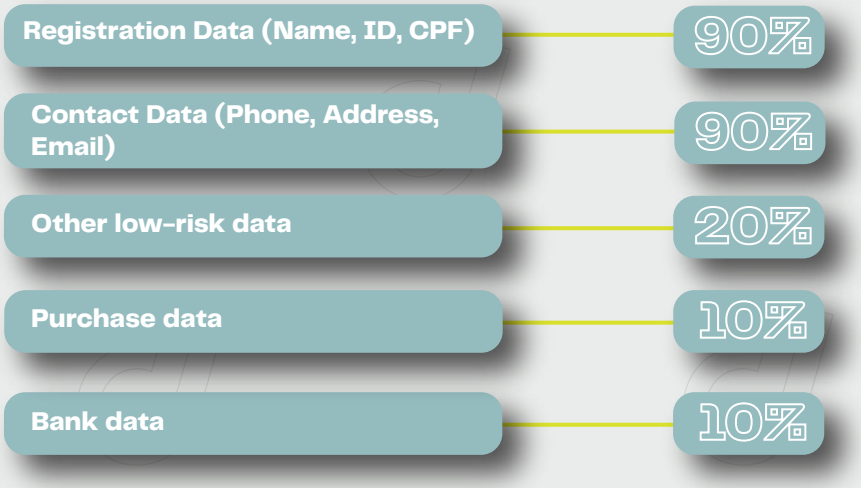
ADVERSE JUDGMENT →

The values ranged from BRL 500.00 to BRL 25,849.00. When the adverse judgment was only for moral damages, the values ranged from BRL 500.00 to BRL 10,000.00. In the case of adverse judgment for pecuniary damages, the variation is greater, ranging from BRL 599.99 to BRL 25,849.00.

LGPD Enforcement in Numbers

Leaked data

In addition, it was identified what data was potentially leaked more frequently within security incidents. In this sense, registration data (such as name, ID, and CPF) and contact data (telephone, address, and email) were the most leaked, being made available in about 90% of incidents.



Facts considered and frequency of adverse judgments

Regarding the outcome of the analyzed decisions, certain tendencies were observed, mainly with regard to the existence or not of an adverse judgment, directly influencing the agent's liability or not.

An example of this would be the finding that in cases where there was an allegation of fortuitous event or force majeure, the adverse judgment is almost certain. On the other hand, it is possible to observe that the public communication of the incident, or communication to the ANPD, the absence of a causal relation with the damage suffered by the plaintiff, as well as the exclusive fault of the data subject or third parties, tend to reduce the chances of adverse judgment.

In re ipsa nature (or not) of moral damage
45% of cases with adverse judgment
55% of the cases without adverse judgment

Type of leaked data
50% of the cases with adverse judgment
50% of the cases without adverse judgment

There was an incident, but there was no proof of a causal relation with eventual damage
100% of the cases without adverse judgment

How the plaintiff became aware of the incident
40% of the cases with adverse judgment
60% of the cases without adverse judgment

Company's public communication about the incident
100% of the cases without adverse judgment

Fortuitous event or force majeure
100% of the cases with adverse judgment

Exclusive fault by a third party
100% of the cases without adverse

Exclusive fault by the data subject
100% of the cases without adverse judgment

Communication to the ANPD
100% of the cases without adverse judgment

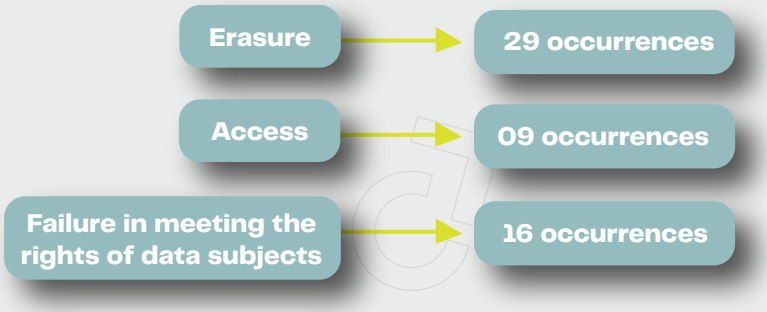
B. Rights of data subjects (article 18 of the LGPD)

Frequency of the topic: rights of data subjects

When analyzing a sample that included ancillary requests, it became clear that discussions involving the right to erasure and generic failures in meeting the rights of data subjects were present, constituting 25% of the analyzed cases.

Furthermore, it was identified that the topics of erasure (64%) and access to information (20%) were the most common within the analyzed theme. Cases of failure in meeting the rights of data subjects regarding their personal data represented 29% of the analyzed cases.

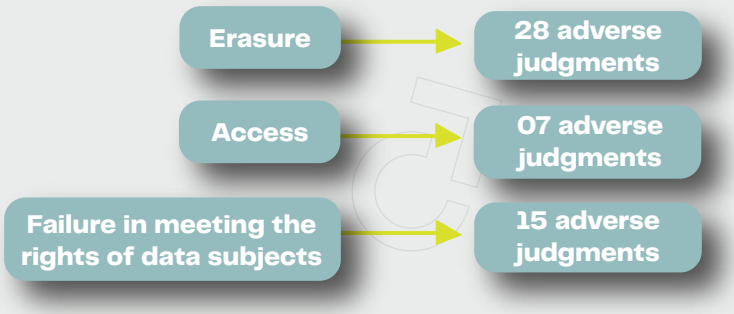
Sample: 45 mentions of data subjects' rights:



Frequency of adverse judgments

Regarding adverse judgments, they occurred frequently.

Sample: 45 mentions of data subjects' rights:



Adverse judgment values

Regarding non-material damages in these cases involving data subjects' rights, the compensations ranged from BRL 500.00 to BRL 15,000.00, specifically for the following variables:

Erasure	From BRL 3,000.00 to BRL 15,000.00
Non-material damages	From BRL 500.00 to BRL 10,000.00
Access	From BRL 4,000.00 to BRL 10,000.00

Regarding pecuniary damages, it was only possible to analyze data related to failures in meeting the rights of data subjects regarding their personal data, as follows:

Failure in meeting the rights of data subjects	From BRL 280 to BRL 25,849

C. Transparency and misuse of personal data

The topics of transparency and misuse of personal data were discussed together, given the frequency of their simultaneous mention in the actions:

Transparency

CONCEPT → Data subjects must be provided with accurate, clear, and easily accessible information regarding the ways, conditions, and details of the processing.

CONCLUSION → A common topic when the situation discussed considers the awareness, on the part of the data subject, about the activity or activities in question.

Misuse of Personal Data

GENERAL CONCEPT → Personal data processing must be conducted in accordance with the purposes informed to the data subject (principle of adequacy). If processing with a purpose other than the one informed occurs, there may be misuse of personal data.

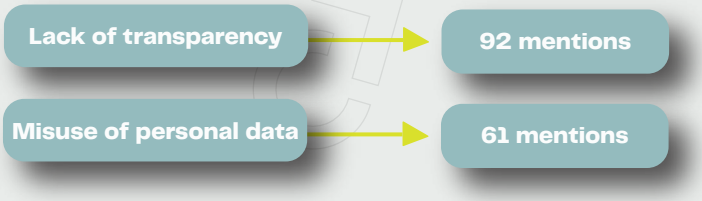
INTERPRETATION IN DECISIONS → The topic is considered when there is identification that personal data has been processed for improper and foreign purposes.

LGPD Enforcement in Numbers

Frequency of occurrences

A significant portion of the processes used in the sample verified that both lack of transparency and misuse of personal data occur with some frequency.

Sample: 177 decisions



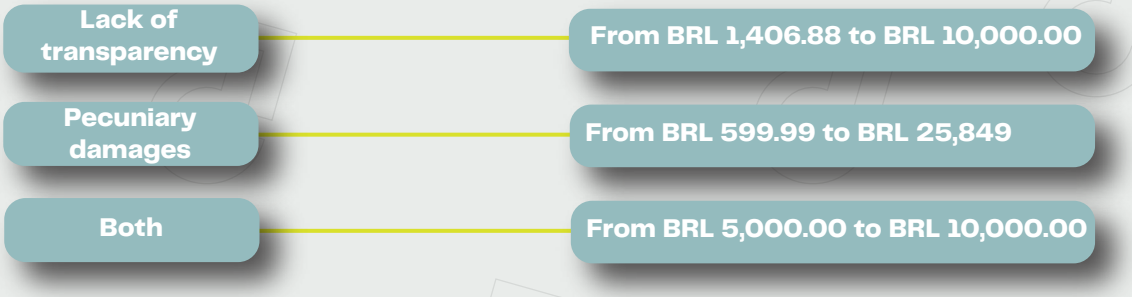
Frequency of adverse judgments

When cross-referencing decisions considering lack of transparency and misuse of personal data with the adverse judgment rate of lawsuits, it is inferred that, despite misuse of personal data having a high chance of generating an adverse judgment, the combination of misuse of personal data with lack of transparency considerably increases these chances. This suggests that the proper application of transparency throughout all processing activities can reduce the chance of adverse judgment by 9%, making the relevance and effectiveness of this type of preventive measure clear.

Lack of transparency	**Misuse of personal data**	**Both**
58% without adverse judgment	18% without adverse judgment	9% without adverse judgment
42% with adverse judgment	82% with adverse judgment	91% with adverse judgment

Values of adverse judgments

There were various variations when considering the minimum and maximum values of adverse judgments



As for adverse judgments for moral damages, there was no significant quantity involving the topic.

Analysis of interpretations

From the aforementioned study, it was also possible to conduct a more in-depth analysis of second instance decisions regarding the in re ipsa nature of moral damages, by observing their different motivations. In addition, the influence of the in re ipsa nature on moral damage awards was also analyzed.

Overall
35% has in re ipsa nature
65% does not have in re ipsa nature

Collection and credit protection
36% has in re ipsa nature
64% does not have in re ipsa nature

Incidents
20% has in re ipsa nature
80% does not have in re ipsa nature

Sharing/Disclosure
55% has in re ipsa nature
45% does not have in re ipsa nature

Thus, it is possible to infer that there is a broader understanding about the in re ipsa nature of moral damages in cases related to the sharing and/or unauthorized disclosure of data, totaling 55% of the analyzed decisions. On the other hand, there is a lower potential in actions motivated by issues related to collection and credit protection, encompassing around 36% of the analyzed cases. Finally, with regard to cases related to security incidents, the observed percentage reached only 20% of the cases.

In re ipsa nature of moral damages in judgments involving security incidents

There is controversy regarding the possible in re ipsa nature of moral damages caused by security incidents, especially when it involves exposure and leakage of data, without the need for proof.

Corpus 1
Moral damages caused by security incidents have an in re ipsa nature

According to this view, the mere incident with personal data (including, in most cases, leaks) is capable, in itself, of causing moral damage. Therefore, it would not be necessary to prove the occurrence and extent of the damage to warrant condemnation for compensation.

Corpus 2
Moral damages caused by security incidents do not have an in re ipsa nature

According to this view, the mere incident with personal data (including, in most cases, leaks) is not capable of causing moral damage. Therefore, it would be necessary to prove the occurrence and extent of the moral damage to warrant an obligation for compensation.

In a recent decision issued on March 7th, 2023 by the Min. Francisco Falcão from the Superior Court of Justice (STJ) in AREsp 2130619/SP it was recognized that material damage resulting from an ordinary personal data security incident (i.e., name, surname, and basic registration information) is not presumed. This means that when the affected data is not classified as sensible data, the data subjects must demonstrate the real damage resulting from the exposure of this information.

In re ipsa nature of moral damages in judgments that cover other situations

In regard to moral damages, the need for proof varies according to the legal fact that generates it. Many judgments, according to the interpretation of the Judiciary, require proof in cases of security incidents, while in other cases, the issue is treated heterogeneously.

Sharing/Disclosure
55% have in re ipsa nature
45% do not have in re ipsa nature

Collections and credit protection
36% have in re ipsa nature
64% do not have in re ipsa nature

Collections and credit protection
Decisions motivated by collections or credit protection require proof of moral damages for indemnity purposes (64%)

Sharing or disclosure
In cases of judgments motivated by sharing or disclosure of personal data, there is a tendency in favor of the understanding that the mere unlawful act is sufficient to warrant compensation for moral damages, although the courts are divided on the subject (55%)

Performance of the ANPD in the administrative sphere

In addition to the abovementioned Lawsuits, the National Data Protection Authority ("ANPD") also supervises companies/organizations to guarantee compliance with LGPD provisions in the administrative sphere.

Among the ANPD's duties, it is worth highlighting the monitoring, guidance, and prevention activities, within the scope of the inspection process which, depending on the outcome, may initiate repressive activity through the Administrative Sanctioning Process.

In exercising its supervisory powers, the ANPD may act (i) ex officio, (ii) as a result of periodic supervisory programs, (iii) in coordination with public bodies and entities, or (iv) in cooperation with personal data protection authorities from other countries, of an international or transnational nature.

The Administrative Sanctioning Process is designed to investigate breaches of data protection legislation within the ANPD's remit, under the terms of article 55–J, IV, of the LGPD, and can be opened (i) ex officio by the General Inspection Coordination, (ii) as a result of the inspection process, or (iii) in the event of a request in which the CGF, after carrying out an admissibility analysis, decides to immediately open a sanctioning process.

We therefore highlight below the main statistics released by the ANPD, which include data up to the third quarter of 2023:

Total number of security incidents reported since January 2021:
733

Total number of requirements received since January 2021:
2646

Concluded inspection processes:
16

Ongoing inspection processes:
13

Inspection Processes that turned into Administrative Sanctioning Processes:
9

Sanctions applied:
3

We will analyze each one separately below:

I. Total of Security Incidents Reported Since January 2021:

Among the reported 733 security incidents, only 274 were categorized in relation to the type of security incident and the number of communications for each type, given that it was only possible to make this information available from January 2023, when the new version of the Security Incident Communication Form began to be used. Therefore, the incidents reported are divided into the following categories:

Computer Virus/Malware	1

Around 40% of information security incident reports concern data hijacking (ransomware), which are attacks/locks on computers in exchange for payment as ransom and return to control of the device. Some measures, such as blocking the addresses of suspicious websites, reviewing security on the devices, and implementing access control to profiles related to your business, among others, can be taken to rule out the possibility of an attack/data hijacking.

II. Total Requests Received Since January 2021

Since January 2021, the ANPD has received 2,646 requests (complaints or petitions from data subjects) requesting enforcement of personal data protection legislation in relation to data subjects.

Petitions are instruments used by data subjects to inform the ANPD of a request submitted to the controller which has not been resolved within the period established by regulation. Complaints are communications made to the ANPD by any person, natural or legal, about an alleged infraction committed against Brazilian personal data protection legislation, other than a data subject's petition.

III. Concluded Inspection Procedures

The ANPD has already conducted and closed 16 inspection cases, as detailed below:

Operation Agents	Analysis Scope	Process n.
DNIT e PRF	Data sharing from DNIT to PRF	00046.000690/2020-22
WhatsApp LLC	Analysis of the Privacy Policy amendment	00261.000012/2021-04
Rebouças/PR City Hall	Disclosure of sensitive data	00261.000565/2021-59
Facebook	Verification of compliance on the processing of personal data	00261.000342/2021-91
Federal Police	Verification of compliance on the processing of personal data	00261.000836/2021-76

LGPD Enforcement in Numbers

Operation Agents	Analysis Scope	Process n.
Telegram Messenger Inc.	Verification of compliance on the processing of personal data	00261.000298/2022-09
Recife/PE City Hall	Verification of compliance on the processing of personal data – Contracting of monitoring and facial recognition	00261.001708/2021-40
Brazilian Federal Revenue	Verification of compliance on the processing of personal data –Ordinance RFB nº 81/2021	00261.001732/2021-89
Digital Govern Secretary	Verification of compliance on the processing of personal data – Technical Cooperation Agreement n. 27/2021 – SGD x Bank Brazilian Association	00261.000043/2022-38
Digital Govern Secretary	Verification of compliance on the processing of personal data – Technical Cooperation Agreement n. 16/2021 – SGD x FEBRABAN	00261.000064/2022-53
Health Ministry	Verification of compliance on the processing of personal data – Data breach of doctor's participating in public hearing data	00261.000079/2022-11
Brazilian Federal Revenue	Verification of compliance on the processing of personal data – Ordinance RFB n. 167/2022	00261.000821/2022-99
Buonny e Open Tech	Verification of compliance on the processing of personal data – Use of personal data for discriminatory purposes	00261.000851/2022-03
Federal Service on Data Processing – Serpro	Technical Cooperation Agreement between Serpro and Drumwave	00261.001457/2022-84

LGPD Enforcement in Numbers

Operation Agents	Escopo da análise	N° do Processo
Ministry of Management and Innovation – Secretariat of Digital Government	Verification of compliance on the processing of personal data – Sharing of personal data between public organizations	00261.002620/2022-26
Municipal Secretariat of Citizen Security (Sesec) of the Municipality of Fortaleza/CE	Verification of compliance on the processing of personal data	00261.002211/2022-20

IV. Ongoing Inspection Procedures

In addition to the processes already concluded, there are currently 13 inspection ongoing processes being investigated by the CGF to verify compliance in the processing of personal data, as detailed below:

Operation Agents	Scope of Analysis	Process n.
Bytedance Brasil Tecnologia Ltda.	Verification of compliance in the children and adolescents processing of personal data	00261.000297/2021-75
Non-identified	Verification of compliance on the processing of personal data of 223 million Brazilian citizens	00261.000050/2021-59
Federal Service on Data Processing – Serpro	Verification of compliance on the processing of personal data – sharing of personal data between public organizations	00261.000704/2021-44
Ministry of Justice and Public Security	Verification of compliance on the processing of personal data	00261.001028/2021-26

LGPD Enforcement in Numbers

Operation Agent	Scope of Analysis	Process n.
Unitfour Tecnologia da Informação Ltda.	Verification of compliance on the processing of personal data	00261.008253/2021-54
Zappo Tecnologia da Informação e Publicidade Ltda.-ME (Contact Pró)	Verification of compliance on the processing of personal data	00261.001709/2021-94
Claro S.A. e Serasa S.A	Verification of compliance on the processing of personal data	00261.000227/2022-06
National Institute of Educational Studies and Research Anísio Teixeira (INEP)	Verification of compliance on the processing of personal data – Changes in ENEM's data policy	00261.000730/2022-53
WhatsApp LLC.	Verification of compliance on the processing of personal data – Sharing of data with the Companies of the Meta Group (Facebook)	00261.001296/2022-29
Nacional Social Security Institute (INSS) e Dataprev	Verification of compliance on the processing of personal data – sharing for the offer of payroll loans	00261.001688/2022-98
Government of the State of Paraná, Company of Information Technology and Communication of Paraná (Celepar) e Algar Soluções em TIC S.A. (Algar Telecom)	Verification of compliance on the processing of personal data	00261.002036/2022-71

Operation Agent	Scope of Analysis	Process n.
Education Center of Media of São Paulo, Uncomplicates, Plus School, Study at home, Explicaê, Manga High e Stoodi	Verification of compliance on the processing of children and adolescents' personal data by digital teaching platforms	00261.001328/2023-77
RaiaDrogasil S.A., Stix Fidelidade e Inteligência S.A. e Febrafar (Brazilian Federation of Associative and Independent Pharmacy Networks)	Verification of compliance on the processing of personal data	00261.001371/2023-32

V. Procedures that became Administrative Sanctioning Processes

By the second quarter of 2023, the ANPD reported the existence of 8 administrative sanction proceedings, as highlighted below:

Proceeding n.	Organization/ Company	Initiated in	Investigated conduct
00261.000456/2022-12	Ministry of Health	7 March 2022	Failure to comply with the ANPD request; absence of a Data Protection Officer; failure to communicate a data breach
261.000489/2022-62	Telekall Infoservice	10 March 2022	Absence of a legal basis for the operation of data; absence of a record of operations; failure to submit a Data Impact Assessment; absence of a Data Protection Officer; failure to comply with the ANPD request

LGPD Enforcement in Numbers

Proceeding n.	Organization/ Company	Initiated in	Investigated conduct
00261.000574/2022-21	Botanical Garden Research Institute of Rio de Janeiro	22 March 2022	Failure to communicate a data breach; Failure to comply with the ANPD request
00261.001192/2022-14	Department of Education of the Federal District	1 June 2022	Failure to comply with the ANPD request
00261.001882/2022-73	Ministry of Health	12 September 2022	Failure to communicate a data breach to data subjects; absence of security measures.
00261.001886/2022-51	Secretary of State of Health of Santa Catarina	17 September 2022	Failure to communicate a data breach to data subjects; absence of security measures; failure to comply with ANPD request.
00261.001969/2022-41	Institute of Assistance to the State Public Servant of São Paulo – IAMSPE	30 September 2022	Failure to communicate a data breach to data subjects; Absence of security measures
00261.001963/2022-73	Secretariat of Social Development, Child and Youth – PE	07 October 2022	Failure to communicate a data breach to data subjects; absence of security measures.
00261.001888/2023-21	National Institute of Social Security – INSS	Not informed	Failure to report a security incident to data subjects and failure to comply with a preventive measure adopted by the ANPD

Some inspection procedures were converted into Sanctioning Administrative Processes to thoroughly investigate cases in which there is an indication that there has been a violation of the LGPD and personal data protection regulations. In cases where there is proof of violations, the ANPD/CGF may apply sanctions.

In March 2023, the ANPD released a list of sanctioning administrative proceedings instituted so far. The list is comprised by public organizations and only one private company, which so far, has been the only one condemned to the application of administrative sanction by the Authority.

VI. Sanctions Applied

To this moment, the ANPD has applied three sanctions, including a fine for non-compliance with the LGPD, after the administrative sanctioning process that was ongoing:

Proceeding n.	Organization/ Company	Penalty/ Warning	Apllied in	Reason
261.000489/2022-62	Telekall Infoservice	R$ 14.400,00	07/06/2023	Processing of personal data without legal basis and lack of proof of a DPO.
00261.001969/2022-41	Institute of Assistance to the State Public Servant of São Paulo – IAMSPE	N/A – Only warning was applied	10/6/2023	Failure to report a security incident to the data subjects; lack of security measures
00261.001886/2022-51	Secretary of State of Health of Santa Catarina	N/A – Only warning was applied	10/18/2023	Failure to prepare a RIPD (Data Protection Impact Report) when requested by the ANPD and failure to report information security incidents to data subjects and to the ANPD

Our recognitions

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 & 2022)

Leaders League (2021 & 2022)

Transactional Track Record (2021 & 2022)

The Legal 500 (2022)

Meet our

Partners

Alan Campos Thomaz

Partner

Technology & Digital Business, Privacy and Data Protection, Fintechs and Intellectual Property

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Filipe Starzynski

Partner

Litigation & Law Enforcement, Civil, Real State, Labor and Family

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Partner

Intellectual Property, Technology, Contracts and Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Follow us

campos thomaz advogados

Subscribe to our newsletter