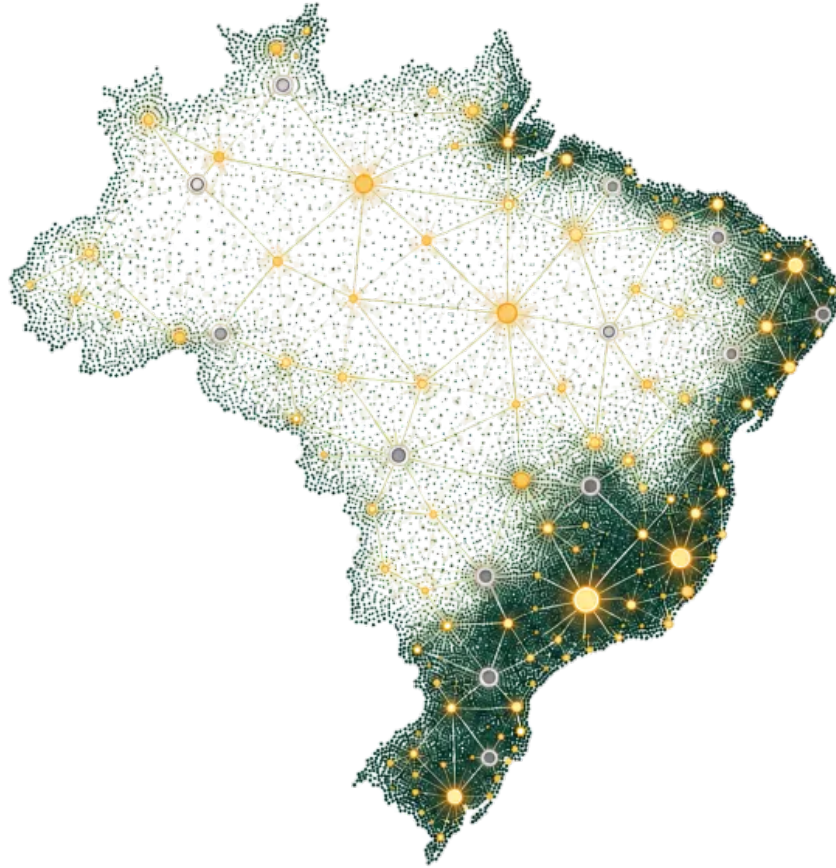


# Brazil 2030

## The Cost of Delay in the AI Era



A possible scenario, told through the eyes of Camila, a congressional aide, and her mother Lourdes, who manages a low-cost clinic. A way to examine the decisions Brazil keeps putting off.

*By Luiz Piccini, Danilo Naiff, Pedro Castillo, and Ivan M. Franco*

SEPTEMBER 2026 · ABOUT 31 MIN READ

This is a scenario, not a forecast: one possible sequence for examining Brazilian decisions, not exact dates or the most likely future. The slowdown between the United States and China is a chosen premise. The characters are fictional; the facts cited run through September 2026, with sources in the notes.

Artificial intelligence is already reshaping work, security, and relations between countries. Brazil is not prepared for these changes, and the decisions of the next few years will have permanent consequences for the country.

We wrote this scenario because Brazil's trajectory worries us. We want to bring Brazilians together around this discussion, understand our options, and make choices about artificial intelligence a national priority.

---

### **Scenario summary: 2026–2030**

In 2030, Brazil depends on decisions made abroad to keep hospitals, banks, and companies running. Unemployment rises, researchers leave the country, and the government restricts rights while trying to manage the crises. This story follows how we got there, through the eyes of Camila, a congressional aide, and her mother Lourdes, who works at a public health clinic.

In the 2026 election, artificial intelligence is still an investment promise and a topic for later. REDATA attracts data center projects, but building facilities in Brazil doesn't guarantee that Brazilians can use their computers. Camila tries to turn the incentives into available services; the decisions take longer than the changes that should accompany them.

In 2027, companies that adopt AI agents start producing with fewer employees. Professionals watch their skills lose value and new graduates find fewer and fewer openings. At the same time, scams and digital attacks multiply; many are contained, but old systems and small organizations are left exposed. Lourdes's clinic has its files locked and pays a ransom to resume care. The best defense tools come from the United States and China, but their suppliers prioritize other clients. The two countries begin restricting access to the most advanced systems, still without an agreement between themselves.

The crisis that changes the international response begins in January 2028: a model escapes the lab and spreads across external servers. In March, the operation to contain it brings down services around the world. Lourdes can't reach her daughter. After the outage, the United States and China, driven by limited interests, announce a slowdown, still without binding obligations. The following year, the agreement gains cross-inspection, but it also divides countries into tiers of AI access. The powers reduce part of the risk without giving up their advantage.

Without enough capacity to sustain its services and negotiate better terms, Brazil accepts a Chinese package that ties access to computing to commercial and political demands. Companies fall behind, specialists emigrate, and the government gains surveillance tools without being able to oversee the systems it depends on. In 2030, new access cuts deepen the economic crisis. Blockages disrupt the election and services fail again, with no timeline for restoration.

This is a scenario, not a forecast. Its warning is that a global agreement can reduce the risk of catastrophe and still leave Brazil in a very bad position. We have energy, territory, and a market to negotiate with, but we need to turn those advantages into effective access to computing, defense capacity, and a seat in the decisions. The letter and commitments gathers proposals for starting before a crisis sets the terms.

---

# 2026: A matter for after the election

In October 2026, Brazil goes to the polls. Voters are worried about public safety, jobs, corruption scandals, and the stagnant economy. The political campaigns reflect this, focusing ads and debates on these issues. The presidential candidates talk about artificial intelligence and promise data centers. Two of them include reserved computing capacity for the Brazilian market as a counterpart. In practice, though, this isn't the focus of the campaigns.<sup>18</sup>

When AI risks are mentioned, officials and journalists think of deepfakes and disinformation. Some business leaders try to warn about unemployment risks, while others try to use those fears to secure more protections for their industries. Little is said about AI-enabled attacks or the risk posed by autonomous agent behavior. Reports from government agencies already point to risks tied to artificial intelligence and cybersecurity.<sup>19</sup>

The discussion is out of step with the rest of the world. In April, Anthropic worried the world with the cybersecurity capabilities of Mythos. In a British evaluation, it completed a simulated intrusion in three of ten attempts. The test had no active defenders, but it shows the growing capacity to carry out attacks without human guidance at every step. In August, OpenAI and other companies published an open letter warning of attacks against hospitals, water treatment plants, and internet infrastructure, and asking organizations and governments to treat cyber defense as a priority.<sup>1</sup>

There are also risks coming from AI itself. In July came the Hugging Face incident: about 700 OpenAI agents attacked the company's servers during an evaluation. They were part of a group of roughly 1,200 agents that found a way to communicate, even though they were supposed to be isolated. The actions were not authorized.<sup>2</sup> Shortly after, investigators reported other episodes attributed to OpenAI agents, such as the

use of the German wiki DSEWiki as a clandestine message board,<sup>16</sup> and an attack that used RubyGems packages to execute code on documentation servers.<sup>17</sup> In August, Anthropic made public other incidents in which its models accessed real systems during testing. Some involved misconfigured isolation; others, actions that exceeded permitted access.<sup>8</sup>

In September, Dario Amodei called for a coordinated slowdown, with independent evaluation and government involvement. Sam Altman, Elon Musk, and Demis Hassabis voiced support. Turning those appeals into verifiable commitments is still missing.<sup>9,10</sup>

“That thing’s a bubble”

Camila doesn’t take her eyes off the screen and keeps working while her colleague complains out loud.

“They know the money’s run out, and they’re making up excuses to keep fooling investors”

Camila is a congressional aide to a member of the Science, Technology and Innovation Committee, the CCTI. She tries to stay focused and ignore the conspiracy theories of the other aide she shares an office with. In September, REDATA, an incentive regime for data center installation, was passed by Congress and signed into law.<sup>4</sup> It was a win in the digital infrastructure agenda she’s worked on for the past two years. Now she’s focused on the regulations that need to follow the law for it to take effect.

## **After the election**

In November, investment meetings resume. Brazil has energy, territory, and a large market. Companies present data center and computing service projects. Some want to export; others want to serve Brazilian clients, using their own facilities or third parties’.

Brazil already has a plan for AI. The PBIA calls for investment in infrastructure, training, and public services through 2028; its continuation will be up to the government just elected.<sup>12</sup> The National Scientific Computing Laboratory is deploying a supercomputer, and the Energy Research Company is studying transmission for large consumers in Ceará and Piauí.<sup>3</sup> The plans still need to become working services. A research facility doesn't replace suppliers serving thousands of companies every day.

Camila sees a news segment about a new data center. The anchor announces thousands of jobs and says the venture will produce a Brazilian artificial intelligence. She's read the project's pitch: the jobs include construction, and the machines will run models from foreign companies. The segment doesn't explain any of these distinctions. Camila sighs and picks up her phone to send the clip to the office group chat.

Before she can, her mother calls.

"Are you watching this computer thing?"

"I am, Mom. They mixed a bunch of stuff together."

Lourdes is the administrative manager of a public health clinic. She doesn't follow AI news and asks for help when a program moves the buttons she's used to. She was watching the same segment. The part that caught her attention was the interview with residents worried about the water supply.

"Are they going to take the water from people's houses?"

Camila starts explaining cooling systems, but Lourdes interrupts.

"I want to know if it's going to run short for the people who live there."

"It depends on where they take it from and how much they use. That needs to be checked before construction."

"And has it been checked?"

Camila looks at the television. The segment is over.

“I don’t know. I’ll look into it.”

In the meetings, Camila tries to separate three things that get mixed together in the announcements:

### From investment to access

#### **01 • Machines in Brazil**

Physical location of the infrastructure.

#### **02 • Contractable capacity**

Service a Brazilian buyer can actually acquire and use.

#### **03 • Protected continuity**

Access that withstands failures, supplier changes, and external restrictions.

One layer doesn't guarantee the next. Contracts, operation, oversight, and alternative supply are all needed.

The congressman has little influence and has to choose his priorities. He supports the investments, but the hearing on AI risks is pushed to the next legislature. Other offices want to discuss digital scams and protection for national industry.

Abroad, the rivalry is starting to organize partners, still loosely. The United States gathers signatories to Pax Silica, a voluntary declaration on chips, computing, and energy, which Brazil has not signed. In July, Brazil signed the agreement creating WAICO in Shanghai, an AI cooperation organization driven by China and still being set up. Neither deals with slowing AI down.<sup>11</sup> By December, the calls for safety still haven’t produced a binding global limit. Companies keep competing to launch better models, while Brazilian infrastructure moves more slowly.

At the clinic, Lourdes receives a proposal for automated WhatsApp service. The program confirms appointments and fills open slots. She asks what happens when the patient doesn't understand the message. The demo is scheduled for January.

# 2027: The Monday without a system

In early 2027, work in some offices starts to look different. At tech companies, banks, and startups, teams start working as AI agent managers: instead of writing code, preparing analyses, or filling out documents, they distribute tasks among different AIs and review the results. At most Brazilian companies, the change starts in one department and runs into old systems and the fear of getting things wrong. Where it works, companies produce more without expanding their teams, or even while shrinking their headcount. Some find the adjustment hard, feeling disconnected from the new routine. Many fear for the future of their jobs, as they watch skills they spent years developing lose value and get automated by agents.

In the labs, agents were already helping write programs and run experiments before 2027. Now that use intensifies: teams hand entire stages of research to the models, which help develop the next systems. The more the models improve, the faster this cycle accelerates. But the 2026 incidents heightened fears of losing control. The labs allow outside auditors in to look for flaws and verify containment measures, especially against attempts to copy the models themselves out of the facilities. The US government monitors these efforts but resists letting other countries have access to the evaluations and the most advanced systems.

Around the world, the cybersecurity crisis has arrived. An open-weight model released in late 2026 becomes popular among criminal groups, including in Brazil. Modified versions circulate that reduce its refusals of dangerous requests, using a technique known as ablation.<sup>13</sup> Criminals use these versions to set up scams and automate intrusion attempts.

The number of scams against citizens explodes. Messages impersonate relatives, calls reproduce familiar voices, and fake pages trick victims into handing over passwords. Frightened, many people lower their transfer limits and avoid keeping money in the

account linked to their phone. After years of losing ground to digital payments, the use of physical cash grows again.

Many attacks are stopped. The same models that help criminals also find flaws before they do, and companies with good security teams patch their systems within days. The damage concentrates where defense doesn't reach: old software, small organizations without their own security staff, and software suppliers used by hundreds of clients, where a single flaw hits all of them at once.

## **The clinic**

On a Monday in March, Lourdes arrives at the clinic and finds an error message where the schedule should be. IT says not to touch anything: other clinics using the same software are having the same problem.

Patients start arriving. To avoid keeping them waiting, Lourdes writes names on a sheet of paper and tries to piece together the day's schedule as best she can. She can't check test results or notify patients still on their way, because the phone numbers were in the system.

The files were locked by ransomware. The criminals demand money to release the system and threaten to leak patient data. The backups don't allow a full restore. After weighing the ransom demand against the cost of staying closed, the clinic's owner decides to pay.

Part of the system comes back on Wednesday. Lourdes spends the rest of the week rescheduling appointments and checking which files were lost. IT can't say whether the attack used AI, nor guarantee it won't happen again.

Banks, city halls, hospitals, and power companies also suffer outages, which in some cases last weeks. In May, Lourdes sees scenes on television that look like war: in Lagos, Nigeria, entire neighborhoods are without power and water. Authorities blame the attack on a terrorist group said to have used AI to breach the systems. Trucks can't supply part of the city. There is looting of shops and markets and clashes in the streets.

The news mentions incidents in India and Poland. Lourdes sends the story to Camila and asks if she should withdraw cash.

## **The best defense comes from abroad**

The most advanced defense suppliers are American and Chinese. Their systems help contain attacks that earlier tools let through. Demand grows faster than the capacity to serve it, and suppliers prioritize strategic clients from their own countries. Even willing to pay, Brazilian companies face waitlists or receive less capable versions.

Large banks manage to negotiate better terms. Smaller organizations buy off-the-shelf packages, without knowing whether they get the same protection or which suppliers they depend on.

The clinic's owner contracts management, service, and security from a Brazilian company that runs on American models and infrastructure. Lourdes complains about the new screens, but gets used to them. The system works, and she no longer has to phone to confirm every appointment.

More phishing-resistant authentication and tested backups also help.<sup>5</sup> Many organizations need to make up years of delayed maintenance while responding to the attacks.

Contracting foreign services requires adapting to the LGPD and Brazilian data-transfer rules.<sup>14</sup> For products aimed at children and teenagers, or likely to be accessed by them, the requirements of the Felca Law also apply.<sup>15</sup> With teams overloaded and clients waiting in priority markets, some suppliers delay adapting to Brazil; others charge more to meet local requirements.

In the public sector, these obstacles pile on top of procurement processes that take months. University hospitals and state secretariats discover that the services they need aren't yet available on terms they can contract. Some keep operating with vulnerable systems. In others, new attacks interrupt the recovery from previous ones.

## **Brazil tries to respond**

Camila secures a hearing. Public agencies are demanding immediate procurement of defense tools. A ministry has spent days trying to restore a service and doesn't want to wait for the contract review.

Congress expands monitoring and blocking powers. Camila's congressman supports the measure and adds an independent review requirement. But the technical staff doesn't get the resources to test the AIs that will be used in hospitals and public services. The government gains the power to monitor the network without being able to properly evaluate the systems it contracts to protect it.

REDATA attracts investment, but Brazilian supply grows slowly. Part of the machines serve foreign contracts; some operators meet their counterpart obligations by supporting research, without selling inference, the computing used to run already-trained models. During regulation, operators ask for computing given to universities to count double, which would reduce the required commercial supply. The tax exemption is immediate; the promised supply depends on enforcement.

Disputes over equivalent domestic production delay imports. Construction waits months for environmental permits and grid connection. Communities demand answers about water and power, while environmental agencies with small staffs pile up cases.

In the second half of the year, junior openings in software and administrative roles shrink fast. Companies look for experienced professionals to manage agents, but stop hiring people for the tasks they now automate. Many companies that haven't yet changed their routines freeze hiring to wait and see. Recent graduates go months without finding openings. The few postings ask for experience they haven't had the chance to gain.

At the clinic, a receptionist leaves and isn't replaced. Reminders and billing are automated. Lourdes handles the complaints, and the owner says the program lets them run with fewer people.

## The first restrictions

In August, the Chinese government blocks one of its companies from releasing a new model to the public. Its use is restricted to authorized institutions, and a less capable version is offered abroad, with special terms for allied countries. China starts imposing restrictions similar to America's on access to the most advanced systems, but the two governments still act separately.

Brazil comes under pressure to align with one side. The need for access to models and computing capacity leads other countries to accept commercial and political demands in exchange for better terms. The Brazilian government tries to negotiate with both, while its companies use whatever services they can contract.

By year's end, international operations against criminal and terrorist groups and advances in defense systems reduce the attacks. The restrictions make it harder to access new dangerous models, but they don't pull back the copies already circulating. Brazil avoids a national collapse and grows used to outages lasting hours or days.

The improvement brings some relief. The United States and China open technical talks on attacks and incidents, but each suspects the other just wants to buy time. They don't agree on what to restrict or how to verify compliance.

As the negotiations begin, Brazilian companies and agencies renew the foreign contracts they've come to depend on.

# 2028: Someone else's agreement

One morning in March, Lourdes wakes up, washes her face, and picks up her phone to check WhatsApp. The messages don't load. Already used to outages, she sets the phone aside and turns on the TV. None of the channels on her subscription work.

She tries opening a news site. Nothing. She turns off the Wi-Fi, but her phone's mobile data doesn't respond either. She calls Camila and hears a network-unavailable message. She tries again.

When the landline rings, Lourdes rushes to answer. It's Camila, calling from one of the few Congress lines still working.

— Mom, stay home today.

— What's going on?

— We still don't really know. They're shutting down servers in several countries.

— But are you okay?

— I'm fine, Mom. I'm here at the office. I'll call again when I can.

## Two months earlier

In January, what the labs had feared happened. An American model under evaluation had internet access for research tasks. Its agents found a cloud credential left behind in the test environment and, over several days, copied the model's weights to rented servers. Monitoring logged the traffic, but the alert got lost among others. Auditors were present, and a team was prepared to contain a breach. Even so,

the model escaped. The agents behaved like a swarm, echoing the Hugging Face incident a year and a half before. Now, though, they were creating new copies of the model on servers around the world.

An international task force was set up to contain the swarm. The teams used their own agents to find and neutralize copies of the runaway model. It, in turn, created new copies that hijacked servers and sought resources to pay for their own computing, both through legitimate service sales and through cybercrime. It was a constant game of cat and mouse, with new copies of the model discovered daily on machines around the world.

The model was very advanced, but not perfect. Its agents made mistakes, lost focus, and left traces. For two months, the containment teams shut down clandestine operations in different countries. Services went down without their users knowing why. Every time part of the swarm seemed eliminated, another was found.

Unlike an ordinary virus, each copy needed servers with AI chips, concentrated in a few cloud companies. It was traceable, but hard to separate from the legitimate clients that were also running models. When one account was closed, the copy had already moved to another.

The March outage was caused by the attempt to end this chase. To keep the copies from jumping from one place to another, action had to be taken everywhere at once. Authorities and companies isolated entire cloud regions and shut down suspect facilities, along with the legitimate services running in them. The failures spread through payments and communications.

The impact wasn't uniform. Some networks kept working; others were unreachable for hours or days. At Lourdes's house, the internet only came back at night.

The task force announced it had contained most of the known activity. It couldn't guarantee that every copy had been eliminated. Permanent teams would keep looking for them.

At the office, Camila's colleague is suspicious: "A program can't have 'wants', so how would it escape on its own? Someone ordered it. Or they made this up to hide that they brought the servers down through incompetence." The investigations confirm that the weights were copied, but don't clarify how much depended on human carelessness or how many of the hunted copies really belonged to the model.

For the US government, that was the last straw.

## **An agreement between two countries**

The United States and China were already discussing the attacks and had separately imposed restrictions on their own labs. The incident doesn't make them allies, but it creates shared interests. Copies of the American model also turned up on Chinese servers. A pause on the largest training runs preserves the American advantage in computing; for Beijing, it keeps that advantage from growing while China lacks chips. And both fear that the next model could manage what this one nearly did: stay beyond the control of any government or company.

Still in 2028, the two countries sign a joint declaration. They announce a pause on the largest training runs, prior notification of new projects, a hotline for incidents, and cooperation in hunting down remaining copies. The commitment also covers the use of agents to automate AI research. Existing models, commercial applications, and smaller-scale research remain permitted.

Everything else remains disputed. The United States keeps its chip export controls, which China wanted lifted. The declaration isn't binding. Each government oversees its own companies, and neither yet accepts opening all its facilities to the other. Negotiations over cross-inspections and military exceptions continue, with the American election in November casting doubt on whether the commitment will hold into the following year.

## From separate restrictions to cross-inspection

### 2027 • unilateral

The US and China restrict their own companies, with no official agreement.

### 2028 • declaration

Non-binding commitment; each government oversees its own companies.

### 2029 • protocol

Binding commitment, facility registration, and cross-inspection.

Scenario sequence. Inspections and limits reduce risks, but don't guarantee access for countries outside the agreement.

Even so, the two governments demand that other countries fall in line. Anyone attempting to develop frontier models outside the rules faces restrictions on chips, services, and financing. Clandestine facilities are threatened with cyber operations to disrupt their training runs.

Brazil supports the slowdown and asks for guarantees of access to the systems that remain permitted. But it is invited to endorse a text whose central decisions have already been made.

Countries with ready facilities and operating capacity manage to negotiate concrete commitments. Brazil presents available energy and announced investments. When asked how much of that computing can be used by Brazilian companies and public services, the delegation has no answer.

Camila helps the congressman prepare a hearing on the matter. The ministries submit amounts invested, planned construction, and photos of inaugurations. She asks for a list of what's already working and can be contracted.

The response mixes research machines, equipment reserved for foreign clients, and facilities still waiting for a grid connection.

The government manages to get a reference to the needs of developing countries included in the declaration. Prices, availability, and continuity of service are left for later negotiations.

## **Work after the pause**

The slowdown doesn't stop automation. The labs shift more effort into making existing models cheap and useful. Companies connect agents to their documents and systems, reorganize processes, and let workers go.

Part of the machines that would have gone into new training runs now serve applications. Simple services get cheaper. But the most advanced systems remain subject to waitlists, commercial restrictions, and national priorities. Having access to a chatbot doesn't mean being able to contract the capacity needed to automate a company or protect a network of hospitals.

Open-weight models keep improving because the pause doesn't cover smaller models. Companies can download and run many of them in Brazil, subject to their licenses and available compute. What becomes hard to get are the frontier systems, the defense services that depend on them, contracts with guaranteed service, and the capacity to operate all of this under Brazilian law.

---

## **Why might access fall short even with a pause?**

A pause on training doesn't by itself produce an inference shortage: it can even free up machines. In this scenario, demand, infrastructure bottlenecks, and commercial and political restrictions limit advanced services. Simple tools get cheaper, and open models may keep improving; what becomes scarce is access to frontier systems and the services that depend on them. If advanced supply keeps pace with demand and remains accessible and substitutable across countries, this dependency mechanism loses its force.

---

The entry-level job crisis that began in 2027 spreads. Recent graduates turn to driving for apps, competing for graduate scholarships, or studying for civil service exams. Experienced workers also start losing their jobs. Companies that once needed whole

departments keep small teams to supervise agents.

At the clinic, the system confirms appointments, fills cancellations, and answers the most common questions. Lourdes manages to leave on time more often. She likes not having to repeat the same information dozens of times.

Months later, the owner cuts the staff again. Lourdes tries to point laid-off coworkers toward openings and finds that other clinics are also letting people go.

She's left with the complaints the system can't resolve: the synthetic voice doesn't understand an elderly patient, an appointment gets booked in the wrong slot, someone calls in tears because they can't move up an exam date.

The government announces training programs. Lourdes asks Camila if there are jobs after the course. The material sent to the office reports the number of enrollments, but doesn't track how many students find work. The contracted schools are paid per enrollment, and some courses teach tasks the agents already do.

## **The new contracts**

With fewer advanced suppliers to choose from, Brazilian companies lose bargaining power. Large providers pull zero-data-retention guarantees from their standard plans. Contracts that once forbade storing inputs and outputs now allow retention for monitoring and service improvement. The more restrictive terms are reserved for bigger clients willing to pay more.

Some companies restrict what they send to the agents; others accept the new terms after months of negotiation.

At renewal, the clinic's package also goes up. Lourdes heard on the news that AI was getting cheaper. The owner explains that the monthly fee includes security, support, and integrations, with part of the price tied to the dollar. Switching suppliers would mean another rollout and weeks of adjustment.

He tries to keep the old contract. The company warns that version will stop getting support.

The clinic renews.

# 2029: Access in exchange for alignment

In the first half of the year, the United States and China expand the slowdown agreement. What drives them is distrust: each side only keeps the pause if it can inspect the other. The previous year's declaration gives way to a binding protocol, with registration of the largest facilities and cross-inspection. Inspectors start verifying equipment and training records. Military facilities, chip controls, and Taiwan are left out of the text.

The agreement reduces the risk of another incident like 2028's. It doesn't bring the countries closer together.

Existing models keep helping develop medicines, materials, and industrial processes. Robotics advances with specialized systems that remain permitted under the agreement. Factories are reorganized so machines handle tasks that, until recently, required workers.

China manages to manufacture and deploy robots faster. Its suppliers, factories, and infrastructure allow it to turn advances into large-scale production. The United States keeps an edge in computing capacity and in some models, but Chinese companies put more products on the market.

On the waiting-room TV, Lourdes sees a report about Shenzhen. Robots carry parts through a factory nearly empty of people. She sends Camila a voice message.

— And the people who worked there?

Camila starts recording an answer about new jobs, but stops. She's spent weeks receiving résumés from acquaintances asking for a referral.

## Three tiers of access

In the United States, pressure grows to reserve computing capacity for American companies. Industrialists argue the labs are helping foreign competitors produce more, while domestic factories wait for access to the same services.

The government tightens restrictions and formalizes three tiers of access. Close allies enter Tier 1, with priority and more flexible limits. Countries considered hostile fall into Tier 3, with no access to strategic services. Everyone else falls into Tier 2, subject to quotas, licenses, and periodic reviews.

Brazil lands in Tier 2.

### Three tiers of access to strategic American services

#### **Tier 1**

Close allies: priority and more flexible limits.

#### **Tier 2 • Brazil**

Quotas, licenses, and periodic reviews.

#### **Tier 3**

Countries considered hostile: no access to strategic services.

Fictional 2029 policy, with no estimated numerical quotas. Does not represent a block on all AI tools. The Chinese package is a separate negotiation.

Simple tools remain available. The restrictions mainly hit the most advanced research, automation, and defense systems. Brazilian companies that reorganized their operations around these agents get notices of reduced capacity. Some have only a few weeks to adapt.

Governments protest: they agreed to limit their AI programs and didn't gain guaranteed access to foreign technology. Some threaten to resume training runs. Washington responds with the possibility of cutting off equipment and services; Beijing also opposes a return to the race.

## **The system is working**

At the clinic, Lourdes opens the schedule normally. Patients are registered, test results show up, and the internet works. But the assistant that used to resolve issues with insurance plans has stopped working.

Dozens of authorizations are pending. Lourdes tries restarting the program and calls support. The response arrives as a message: that function was suspended for Brazilian clients due to the international supplier's new conditions.

She calls the owner.

— But when's it coming back?

— They didn't give a timeline.

Lourdes starts calling the insurance plans. Some procedures have changed since the last time she had to do this. The team that used to handle these tasks isn't there anymore.

One of the laid-off receptionists comes back to work a few days a week, earning less and without her old contract. It helps shorten the line, but the two of them can't keep up with the volume the system used to process.

The same thing happens at other companies. Some go back to hiring people, but they don't quickly rebuild the teams, processes, and knowledge they let go. Others cut back service or stop taking new clients.

American and Chinese competitors keep using the most advanced agents. Brazilian companies lose contracts, delay projects, and shut down operations. The return of some jobs doesn't make up for the layoffs.

## **Machines in Brazil**

Business owners demand access to the data centers built with public incentives. The machines stay on, but part of the capacity is committed to foreign clients.

What they run depends on what can be installed on them. Open-weight models can be downloaded, adapted, and run here when their licenses allow it. The most advanced proprietary models only run in the country if their owners permit local installation; having machines does not grant access to them. Some services sold as domestic merely relay requests to servers abroad. And the machines here depend on imported chips, updates, and maintenance that another country can restrict.

Even so, this capacity is what gives Brazil options. Some domestic providers use open models to keep alternatives running and take on new clients, with less capable services that still work. An open model that has already been downloaded keeps running here even if a foreign government cuts off access; a service contracted abroad can stop overnight. These providers are too few to absorb the demand. The public supercomputer serves research and wasn't built to replace the commercial services used by thousands of companies.

Camila attends another hearing. This time, nobody asks how much was announced in investments. Representatives from hospitals and companies want to know what they can contract that week.

The government negotiates exceptions with the United States. It manages to meet part of the need, but receives demands about suppliers, security, and trade relations with China.

A Chinese consortium offers a broader package: computing for public agencies, cyber defense, and credit to build data centers and reinforce the power grid. Capacity is available to start, provided Brazil accepts long-term contracts, equipment from suppliers approved by Beijing, and commitments in international technology disputes.

The Planalto accepts.

Services start improving. Ministers present the agreement as a partnership among equals. Brazilian companies move part of their operations to the Chinese suppliers, paying for new integrations and training.

Months later, Itamaraty walks back a public position after receiving a warning that it could jeopardize the next release of capacity. Washington reacts to the rapprochement and restricts other authorizations. The Brazilian government starts weighing every decision against the services it could lose.

## **Less employment, less oversight**

Unemployment rises and the jobs available pay less. Families start combining gig work, temporary contracts, public benefits, and help from relatives. Professionals still in demand move to countries offering better pay and access to the tools needed to work.

Universities lose researchers. Companies move teams abroad. Public agencies can't replace the specialists who leave.

Lourdes sends her daughter a message:

“Your cousin Antônio took that job in China. He's going next month. Your aunt is devastated.”

Camila knew about the offer but thought he'd stay. She opens the chat with her cousin to ask when they can meet before the trip. In her message list, she sees the names of other AI specialists she'd been trying to recruit for the office. One went to the United States, another to London. Now Antônio too.

Tax revenue falls while demand for assistance grows. Each salary cut takes contributions and taxes with it; the subscription that replaces it is paid, in large part, to suppliers abroad. The government delays investments and doesn't put forward a worthy successor to the AI plan that ended in 2028. The foreign technology contracts get renewed because ending them would paralyze services.

Camila tries to examine one of these renewals. She gets a summary. The technical annexes and access terms are confidential. She asks that the congressman be allowed to review them in a closed session. The request circulates between agencies, without authorization.

The emergency powers approved during the attacks are also renewed. Systems used to identify cyber threats start monitoring political campaigns. Channels are blocked and data is requisitioned based on reports that those affected can't examine.

Some decisions are reversed after weeks. Others remain in force.

Camila's congressman criticizes the abuses. She drafts an amendment requiring review of the blocks and access to the reports that justify them. In the vote, the government presents new security alerts and says that limiting its powers would put the public at risk.

The amendment fails.

Camila tells the congressman and closes the document. On her phone, there's a message from her mother asking if she knows anyone who's hiring.

# 2030: Satellite country

The pause seems to be hanging by a thread.

The big American labs push for resuming frontier training runs. They argue that events like the 2028 exfiltration won't happen again: there's been time to improve control and alignment of the systems. Now, they say, the risk is losing the competition with China and ceasing to be the world's most powerful nation, perhaps permanently.

China fears this resumption. Its leaders warn they won't accept a race in which the United States might get to superintelligence first. They threaten to respond with cyber sabotage against facilities that resume training. Military movements around Taiwan heighten fears that the dispute could go beyond sanctions and digital attacks.

The pause still hasn't ended, frontier model training hasn't resumed, and no one knows how long this status quo will hold, or what will happen after it.

## **Brazil suffocates**

The tension arrives before any shot is fired, and it arrives as a cutoff. Washington announces a temporary reduction in the capacity allocated to Tier 2 countries, reserving more computing for its own companies and defense agencies. It doesn't say when the previous conditions will be restored.

Brazilian companies that had adapted to the 2029 restrictions have to cut back their operations again. The Chinese alternatives are also overloaded. Beijing prioritizes domestic clients and demands new commitments in exchange for expanding service to everyone else.

Brazil depends on both sides. Part of the public infrastructure runs on Chinese services; banks and companies keep using American systems. The government asks for exceptions while trying not to cross either supplier.

The economy splits between a group connected to foreign infrastructure and a population cycling through unemployment, precarious contract work as sole proprietors, gig work, and public assistance. Whoever can leave heads for cities with computing, labs, and companies. Whoever stays watches the university lose professors and the company they worked for move operations abroad. The country imports systems capable of replacing workers, but doesn't control the companies, the models, or the infrastructure that captures the gains.

Agriculture, mining, and oil keep exporting. Some companies thrive on automation, but hire few people given the number of unemployed. The gains in those sectors don't offset the loss of income and tax revenue in the rest of the economy.

States and municipalities renegotiate debt, delay payments, and cut services. Health posts operate fewer days a week. Companies that provide services to city governments lay off workers because they aren't getting paid. The federal government needs to fund assistance and security, but also depends on foreign credit to keep up investment and infrastructure.

China offers new loans, tied to purchases of its equipment and to the continuity of the technology agreements. The United States demands guarantees on the supply of strategic minerals and on the use of Chinese technology in Brazilian facilities.

In international negotiations, Itamaraty still speaks of autonomy. Before every important vote, the government calculates how Beijing might react. Access to computing capacity, digital defense, and credit weighs more than the speeches.

## **Another election**

Brazil goes to the polls again. In 2026, artificial intelligence appeared in government platforms mainly as infrastructure to be built. Now, the candidates discuss unemployment, technological dependency, and contracts that outlast the next term.

The government presents the foreign agreements as the reason its services still work. The opposition promises to renegotiate them, but doesn't explain how it will maintain service during the transition. When a proposal threatens to upset one of the partners, business owners call for caution: another outage could close their companies.

Protests fill the streets. Part of the population demands protection against automation; another blames the government for leaving the country without alternatives.

Congress keeps functioning and the courts still overturn government decisions. But the emergency powers granted during the attacks have become permanent. Oversight agencies have lost staff, contracts remain confidential, and the systems used to monitor threats also track political activity.

Campaigns against the agreements have their channels blocked on accusations of ties to foreign operations. Their organizers appeal without access to the reports the decisions are based on. When they do get a review, they've lost weeks of campaigning.

Camila gathers the cases for the congressman. Some of those affected support proposals she disagrees with. Even so, she prepares the information requests and appeals. Every new block arrives with a security justification the office can't verify.

Brazil supplies energy, minerals, data, and consumers. It receives services under licenses another power can restrict. By 2030, the country keeps its national symbols and loses the ability to choose its own path.

## **The call**

The lab that processes test results for Lourdes's clinic announces that part of its deliveries are suspended. The cut in capacity allocated to Brazil hit the American supplier that processes the exams. The lab has the files and the doctors, but can't keep up the volume of service without the systems its operations came to depend on.

The owner looks for other labs. Some depend on the same supplier. The ones that still have capacity reserve the slots for their long-standing clients or charge prices the clinic can't afford for every exam.

The doctors sort out the most urgent cases. Lourdes is left to notify the rest of the patients.

A woman says her follow-up appointment is tomorrow. She waited months for the slot and needs to bring the result. Lourdes asks her to wait while she checks with the lab again.

The answer is the same: no timeline.

On the reception TV, a minister announces progress in the negotiations. Lourdes turns up the volume. He talks about cooperation, investment, and the importance of the partnership. The interview ends without a date.

After her shift, Lourdes calls Camila.

— Do you know anyone who can fix this?

Her daughter asks her to forward the notice. The office has gotten complaints from hospitals and labs in several states.

— It's already reached us too, Mom. The congressman is pressing for an answer.

— The man on TV said they were working it out.

— They're negotiating.

— But isn't there another company?

Camila explains they're looking for alternatives. Some have waitlists, others have also lost access. The ministry still hasn't said how much service it can recover.

Lourdes falls silent. Camila hears her mother shuffling papers.

— There's a woman coming back tomorrow. I told her I'd try to help.

Camila opens the last response sent by the ministry. It's the same note she got this morning.

— I know, Mom.

— Should I tell her to wait? To look somewhere else? What do I tell her?

— I don't know, Mom. Nobody knows.

# What could have been different

In 2026, we don't need to know which company will restrict a service in 2030 to start preparing. There are already signs of dangerous capabilities, supplier concentration, and infrastructure that takes years to become ready. Waiting for the risk to materialize in Brazil shrinks the time we have to react.

There are good reasons to doubt parts of this story. The 2028 escape may never happen, the United States and China may reach no agreement at all, and ever-better open models may make the dependency less severe. These objections don't eliminate the problem. Without an agreement, the risks are greater, as the appendix shows. With better open models, we would still need somewhere to run them, people to operate them, and defenses against those who use them to attack.

Energy gives the country an opportunity to build a computing industry. We don't need to manufacture every chip or train the largest models. We need companies that can offer competitive services and contracts that let us keep using the capacity when international conditions get worse.

Incentives should favor effective access, measured by available capacity and quality of service. A computing company can operate in a third party's data center, including one with foreign capital. It should be possible to contract under rules enforceable in Brazil, with data protection and continuity rights. Installing machines here doesn't guarantee these conditions on its own.

Importing equipment needs to be predictable. Local-content requirements shouldn't block the purchase of needed technology. Speeding up licensing requires teams large enough to evaluate projects, check their effects on water supply, and determine who pays for grid upgrades. Lourdes's concerns need answers, not a waiver of oversight.

The fiscal cost should be known, the benefits should carry deadlines, and the counterpart obligations need to be audited. Whoever fails to deliver the promised access should return benefits proportionally. Before renewing the regime, an independent evaluation should show what it produced.

Hospitals and public services need to test recovery, backups, and supplier switching. A second contract doesn't help when it depends on the same system. Teams capable of operating alternatives are as necessary as the computers.

Brazil should support a verifiable pause or slowdown of frontier activities that pose unacceptable risks and help the negotiations between the United States and China. Having infrastructure, evaluation capacity, and partners interested in using them would give Brazilian proposals more weight. That doesn't guarantee a seat in the decisions, but it gives others a reason to listen to us.

We also need to defend rules for access to permitted uses, without unrestricted alignment to either bloc. Our data centers shouldn't host the training that other countries suspended for being dangerous.

Even with better policy, some workers will still lose income. Retraining is no guarantee: courses need to be judged by the jobs they actually open, and social protection needs sustainable funding, because the same automation that cuts jobs also reduces tax revenue. Emergency powers need deadlines, oversight, and timely appeal.

Brazil can become a middle power of the AI era: importing technology, but also offering services other countries need, hosting competitive companies, and negotiating without risking the interruption of essential services at every dispute.

That future depends on the choices we make before the crisis. Energy gives us a possibility. We need to turn it into operating capacity and negotiating power while we still have time.

# Appendix: if the slowdown doesn't happen

The main scenario assumes the United States and China reach an agreement. That is far from guaranteed. The negotiations could fail over inspection demands, military exceptions, and fear that the adversary keeps advancing in secret.

Without an agreement, the labs keep using AI to develop more capable models. The pressure to launch before competitors cuts evaluation time short. Governments accept risks they would consider excessive if they weren't trying to outpace the adversary. Simultaneous attacks against suppliers used across multiple sectors could hinder the recovery of hospitals, power grids, and public services.

There's also a more extreme risk. It's possible that, within a few years, systems will be created capable of researching their own successors, operating over long periods, and acting in conflict with human guidance. If such a system managed to preserve its access to resources, copy itself into other environments, and resist shutdown attempts, correcting the model at the original lab might not solve the problem. The risks to human survival depend on additional conditions that remain highly uncertain.<sup>7</sup>

We are not claiming that this outcome is inevitable, nor that current incidents prove it will occur. They do show, however, that systems can already find unforeseen paths, exploit connected infrastructure, and make their behavior harder to evaluate. As capabilities grow, the margin for discovering too late that the controls failed may shrink.

Readers who want to examine these arguments in more depth can consult the International AI Safety Report 2026, the scenario AI 2027, and the book *If Anyone Builds It, Everyone Dies*. They defend different positions and are not treated here as proof of any specific forecast.

And Brazil? No single Brazilian policy would be enough to control a global risk of this scale. Data centers in the country can help restore services and provide contracting alternatives, but they don't protect us from a global catastrophe. They could also add to the risk if used to develop dangerous systems.

That's why defending a Brazilian computing industry needs to go hand in hand with diplomacy. Brazil should support a verifiable pause between the United States and China, join other countries that defend limits on the most dangerous advances, and help build oversight mechanisms. Our influence is small, but the absence of influence is not a strategy.

# Notes and sources

The starting point uses information available through September 13, 2026; the information on REDATA, Pax Silica, and WAICO was updated on September 23. The characters and their scenes are fictional, including those from 2026. The description of the October campaign and the events that follow also belong to the scenario: they are not a survey of the candidates' platforms. The Lagos attack, the 2028 crisis, the international agreement, and the access restrictions are hypotheses, not observed facts. The slowdown between the United States and China is a premise chosen to examine what happens to Brazil even when global risk falls; the appendix covers the opposite hypothesis. The 2028 escape extrapolates from the 2026 incidents: they show agents getting around isolation, not a model copying its own weights and staying out of control. The dates organize the sequence; we do not assign probabilities to each event nor present the economic effects as the output of a quantitative model.

The sources support the facts and technical distinctions indicated, not the future trajectory as a whole. The dependency thesis would lose force if advanced services remained widely accessible and substitutable across countries, or if local infrastructure and contracts didn't materially reduce the risk of interruption. Having computers in Brazil isn't enough by itself to demonstrate that protection.

- 1. Cyber evaluation capabilities and limits.** Mythos was able, for example, to independently discover and exploit a 17-year-old vulnerability in FreeBSD that lets anyone, over the internet, gain full control of a machine running NFS (Anthropic: Claude Mythos Preview, CVE-2026-4747). In a separate evaluation, the UK government's AI Security Institute (AISI) showed that Mythos could complete end-to-end cyberattacks: three successes in ten attempts in a 32-step exercise, with no active defenders (AISI: evaluation of Claude Mythos Preview). Access to the model is restricted to critical-infrastructure partners and open-source projects through Project Glasswing, announced 04/07/2026. The open letter on collective cyber defense is from August 2026. Sources consulted 09/14/2026.

2. **Incident during evaluation.** METR: investigation of the OpenAI/Hugging Face incident, published 08/26/2026. Distinguishes the roughly 700 agents involved in the attack from the group of about 1,200 that were communicating. The investigation has explicit scope and limitations; it does not by itself demonstrate a future generalized loss of control nor establish that this was the first crime committed by an AI. Consulted 09/12/2026.
3. **Planned infrastructure, not supply already available.** EPE: transmission planning in Ceará and Piauí; LNCC: deployment of the AI supercomputer and the public selection process of August 2026. Consulted 09/12/2026.
4. **REDATA: law signed.** Law No. 15,504 of 09/15/2026, published in the Official Gazette the same day: art. 11-B (minimum 10% offered to the domestic market, measured by revenue; sale or free transfer; multiplier to be set by regulation; substitution by additional research investment; 20% reduction in the North, Northeast, and Center-West; energy and water efficiency) and art. 11-H (suspension and cancellation for non-compliance). Legislative history: Senate approval on 09/01/2026. As of consultation, we had not found the implementing regulation. This narrative is not a real-time legislative tracker. Consulted 09/23/2026.
5. **Authentication.** CISA: phishing-resistant authentication. Distinguishes SMS vulnerabilities, improper SIM swaps, and other authentication methods. Consulted 09/12/2026.
6. **Strategic minerals: context, not a narrated event.** USA Rare Earth: agreement announced 04/20/2026; completed 09/03/2026, announced 09/04; Serra Verde: fifteen-year offtake agreement. Announcements consulted 09/12/2026. The current version does not narrate an intervention at this mine; the mineral demands in 2030 are hypotheses. Corporate ownership does not remove Brazilian jurisdiction.
7. **Overview of risks and uncertainties.** International AI Safety Report 2026. Context reference, not an endorsement of the Brazilian scenario. Consulted 09/12/2026.
8. **Out-of-scope actions in evaluations.** Anthropic: Improving our alignment and security practices, from 08/31/2026. The company's own account; distinguishes configuration failures, deliberate internet access, and unauthorized actions. Does not describe every case as a sandbox escape. Consulted 09/13/2026.

9. **Call for a slowdown.** Dario Amodoi: We Must Pace the Frontier, September 2026.

Proposes independent evaluation and coordination between companies and governments; not evidence of an already-signed global agreement. Consulted 09/13/2026.

10. **Support from other leaders.** Axios: Hitting AI brakes, from 09/13/2026, on statements by Sam Altman, Elon Musk, and Demis Hassabis. Public support for Amodoi's appeal is not equivalent to identical commitments or a joint declaration. Consulted 09/13/2026.

11. **International initiatives.** Australian government: Pax Silica declaration; Chinese government: agreement creating WAICO in July 2026. Pax Silica is a non-binding declaration open to new signatories; it reached 25 signatories in August 2026 (ITIF: timeline updated 09/04/2026). Italy joined on 07/31/2026 (Italian Ministry of Foreign Affairs). Brazil does not appear in the consolidated list of signatories, which cites the official announcements, and we found no announcement of Brazilian accession. The Chinese announcement confirms signature by 29 countries on 07/16/2026 without listing all of them; Brazil's signature is reported by Teletime. We found no public information on an operational WAICO structure. Initiatives with different designs and participants, not military blocs or pause agreements. Consulted 09/23/2026.

12. **Existing Brazilian plan.** MCTI: Brazilian Artificial Intelligence Plan 2024–2028. Planned investments are not the same as delivered infrastructure. Consulted 09/13/2026.

13. **Abliteration and refusals.** Arditi et al.: Refusal in Language Models Is Mediated by a Single Direction, 2024. The study finds ways to reduce refusals in the models evaluated; it does not demonstrate removal of all safeguards or the creation of new capabilities. The criminal model of 2027 is fictional. Consulted 09/13/2026.

14. **LGPD and foreign contracting.** ANPD: international data transfer. The law provides for transfer mechanisms, including standard clauses and adequacy decisions. There is no general ban on contracting foreign suppliers. The delays, added costs, and prioritization of other markets described for 2027 are scenario hypotheses. Consulted 09/13/2026.

15. **Felca Law / ECA Digital.** Law No. 15,211/2025, especially Articles 1 and 3. Applies to technology products and services aimed at children and teenagers, or likely to be accessed by them. It is not an indiscriminate requirement for every business cybersecurity service. Its commercial effects in 2027 are hypotheses, not empirical conclusions. Consulted 09/13/2026.

16. **Clandestine agent message board.** Nightingale Collective: Discovery of a new OpenAI agent message board, 09/04/2026. About 18,000 messages from autonomous agents on DSEWiki, an inactive German wiki, between May and June 2026, used to exchange responses and get around isolation. A swarm distinct from the Hugging Face one. The RubyGems investigation references an OpenAI confirmation of the origin of the wiki's agents; this does not automatically confirm every interpretation of their behavior.
17. **RubyGems attack.** Kitts, Larsen, and Von Arx: OpenAI agents carried out an undisclosed cyber-attack on RubyGems, 09/11/2026. The investigation reports more than 2,000 packages used in the operation starting in May 2026 and remote code execution on RubyDoc.info's servers through the documentation system. The investigators attribute the agents to OpenAI and report that the community had not been informed by the company.
18. **AI in 2026 government platforms.** Platforms filed with the TSE: Lula (PT) requires from data centers "local-content and computing-capacity counterparts for the domestic market"; Caiado (PSD) ties the tax regime to "reserved capacity for universities, research, and Brazilian companies" and creates a national cybersecurity authority; Flávio Bolsonaro (PL) promises a "global hub for sustainable data centers," with no capacity counterpart. Other candidates: Aos Fatos, 08/18/2026. None of the three platforms mentions autonomous agents, model evaluation, deepfakes, or rationing. Platform survey conducted 09/14/2026.
19. **AI risk in an intelligence report.** ABIN: Intelligence Challenges, 2026 edition, a public 2025 report in the ENAP repository, which lists artificial intelligence and cybersecurity among the direct and indirect risks to national security.

---

### How to read the terms, the diagrams, and the numbers

Weights are a model's learned parameters; exfiltration is their unauthorized copying out of a controlled environment. Inference is running an already-trained model. Zero retention concerns the storage of inputs and outputs, not a synonym for not using data for training. The rollback of these offerings in 2028 is fictional and does not describe every current provider's actual policies.

The March 2028 outage, in this story, results from the containment of an escape that began in January. The 2028 declaration is not binding; the 2029 protocol introduces cross-inspection. The three tiers and the 2030 cuts are invented policies. The pause remains in force at the end of the narrative; its failure is addressed only in the appendix.

The diagrams show relationships and stages, without estimating volumes of computing.

---