EVIDENCE

OTTAWA, Thursday, April 30, 2026

The Standing Senate Committee on Social Affairs, Science and Technology met with videoconference this day at 10:32 a.m. [ET] to examine and report on matters related to the impact of artificial intelligence in Canada; to consider Bill S-5, An Act respecting the interoperability of health information technology and to prohibit data blocking by health information technology vendors; and, in camera, to consider a draft report.

Senator Rosemary Moodie (*Chair*) in the chair.

[*English*]

The Chair: My name is Rosemary Moodie. I'm a senator from Ontario and the chair of this committee.

Before we begin, I would like to ask all senators to consult the cards on the table for guidelines to prevent audio feedback incidents. Please make sure to keep your earpiece away from microphones. Do not touch the microphones. Activation and deactivation will be managed by the console operator. Finally, please avoid handling your earpiece while your microphone is on.

Earpieces should either remain on the ear or be placed on the designated sticker at each seat. Thank you for your cooperation.

Now, I would like to do a round table and have senators introduce themselves.

Senator Burey: Good morning, everyone. I am Sharon Burey, senator from Ontario.

Senator Senior: Paulette Senior, senator from Ontario.

[*Translation*]

Senator Boudreau: Victor Boudreau from New Brunswick.

[*English*]

Senator Hay: Katherine Hay, Ontario.

Senator Arnold: Dawn Arnold, New Brunswick.

[*Translation*]

Senator Petitclerc: Chantal Petitclerc from Quebec.

TÉMOIGNAGES

OTTAWA, le jeudi 30 avril 2026

Le Comité sénatorial permanent des affaires sociales, des sciences et de la technologie se réunit aujourd'hui à 10 h 32 (HE), avec vidéoconférence, pour étudier, afin d'en faire rapport, les questions relatives aux répercussions de l'intelligence artificielle au Canada; d'étudier le projet de loi S-5, Loi concernant l'interopérabilité des technologies de l'information sur la santé et visant à interdire le blocage de données par les fournisseurs de technologies de l'information sur la santé; et, à huis clos, d'étudier une ébauche de rapport.

La sénatrice Rosemary Moodie (*présidente*) occupe le fauteuil.

[*Traduction*]

La présidente : Je m'appelle Rosemary Moodie. Je suis sénatrice de l'Ontario et présidente de ce comité.

Avant de commencer, je voudrais demander à tous les sénateurs de consulter les fiches posées sur la table devant eux pour prendre connaissance des consignes visant à prévenir les incidents de rétroaction acoustique. Veuillez vous assurer de tenir votre oreillette en retrait des microphones. Abstenez-vous de toucher aux microphones. Ces derniers seront activés et désactivés par l'opérateur de la console. Enfin, veuillez éviter de manipuler votre oreillette lorsque votre microphone est allumé.

Les oreillettes doivent être gardées à l'oreille ou être déposées sur l'autocollant prévu à cette fin correspondant à votre place. Merci de votre coopération.

Je voudrais maintenant faire un tour de table et demander à mes collègues de se présenter.

La sénatrice Burey : Bonjour à tous. Je suis Sharon Burey, sénatrice de l'Ontario.

La sénatrice Senior : Paulette Senior, sénatrice de l'Ontario.

[*Français*]

Le sénateur Boudreau : Victor Boudreau, du Nouveau-Brunswick.

[*Traduction*]

La sénatrice Hay : Katherine Hay, de l'Ontario.

La sénatrice Arnold : Dawn Arnold, du Nouveau-Brunswick.

[*Français*]

La sénatrice Petitclerc : Chantal Petitclerc, du Québec.

[*English*]

Senator Cardozo: Good morning. Andrew Cardozo, Ontario.

Senator Cuzner: Good morning. Rodger Cuzner, Nova Scotia.

The Chair: During the first portion of our meeting today, the committee will continue its study on matters relating to the impact of artificial intelligence in Canada. This study will examine issues such as data governance and sovereignty, ethics, privacy, safety, risks, benefits and social impact of artificial intelligence in Canada.

Joining us today for the first panel, we welcome the following witnesses: Alexandra Dassa, Senior Vice President, Technical Success and Value Engineering, Coveo; John Menezes, President and Chief Executive Officer, Bell Cyber Inc., Bell Canada; and Michel Richer, President, Bell AI, Bell Canada.

Thank you for joining us today. For your opening statements, you will each have five minutes, followed by questions from committee members. Ms. Dassa, the floor is yours.

Alexandra Dassa, Senior Vice President, Technical Success and Value Engineering, Coveo: Good morning, chair and honourable senators. Thank you for the invitation to appear before you today.

My name is Alex Dassa. I am the senior vice president of technical success and value engineering at Coveo, a leading and profitable Canadian enterprise AI company operating globally.

I am here to speak to one central idea: AI sovereignty is not theoretical for Canada; it is an economic, strategic and national imperative.

Sovereignty, in simple terms, means one thing: Nobody can turn off Canada, and no one can compel or force a Canadian company or institution to hand over data, except a Canadian court of law. But AI is not one thing. It is a stack of technologies with multiple layers. So the real question is not whether Canada participates in AI. Rather, it is this: Where do we choose to focus and where can we actually win? That is because we cannot own every layer.

Take frontier AI model development, for example. The level of investment required is clearly prohibitive. It is measured in the hundreds of billions of dollars. Canada will not get economic

[*Traduction*]

Le sénateur Cardozo : Bonjour. Andrew Cardozo, de l'Ontario.

Le sénateur Cuzner : Bonjour. Rodger Cuzner, Nouvelle-Écosse.

La présidente : Au cours de la première partie de la séance d'aujourd'hui, le comité poursuivra son étude sur les questions relatives aux répercussions de l'intelligence artificielle au Canada. Nous nous pencherons donc sur des enjeux tels que la gouvernance et la souveraineté des données, l'éthique, la protection de la vie privée, la sécurité, les risques, les avantages et l'impact social de l'intelligence artificielle au Canada.

Notre premier groupe d'experts de la journée réunit les personnes suivantes : Alexandra Dassa, vice-présidente principale, Expérience client et ingénierie de la valeur, Coveo; John Menezes, président et chef de la direction, Bell Cyber Inc., Bell Canada; et Michel Richer, président, IA Bell, Bell Canada.

Merci de vous joindre à nous aujourd'hui. Vous disposerez chacun de cinq minutes pour vos déclarations liminaires, qui seront suivies de questions des membres du comité. Madame Dassa, vous avez la parole.

Alexandra Dassa, vice-présidente principale, Expérience client et ingénierie de la valeur, Coveo : Madame la présidente, honorables sénateurs, bonjour. Je vous remercie de m'avoir invitée à comparaître devant vous aujourd'hui.

Je m'appelle Alex Dassa. Je suis vice-présidente principale de la réussite technique et de l'ingénierie de la valeur chez Coveo, une entreprise canadienne de premier plan et rentable qui se spécialise dans l'intelligence artificielle d'entreprise et œuvre à l'échelle mondiale.

Je suis ici pour vous parler d'une idée centrale, à savoir que la souveraineté en matière d'intelligence artificielle, ou IA, n'est pas une notion théorique pour le Canada, mais bien un impératif économique, stratégique et national.

En termes simples, la souveraineté signifie une chose : personne ne peut « éteindre » le Canada, et personne ne peut contraindre ou forcer une entreprise ou une institution canadienne à communiquer des données, à l'exception d'un tribunal canadien. Or, l'IA n'est pas une entité monolithique. C'est un ensemble de technologies opérant à plusieurs niveaux. La vraie question n'est donc pas de savoir si le Canada doit prendre part à l'IA. Elle est plutôt la suivante : comme nous ne pouvons en maîtriser toutes les couches, sur quoi devrions-nous jeter notre dévolu et quels sont les aspects où nous pouvons réussir?

Prenons l'exemple du développement de modèles d'IA de pointe. Le niveau d'investissement requis est clairement prohibitif. Il se chiffre en centaines de milliards de dollars. Le

value or even strengthen its position by trying to outspend others on frontier models.

That said, Canada should absolutely continue to invest in research. We have world-class talent and have contributed meaningfully to global AI advancement.

Too often, however, that talent is not deployed here at home in the service of Canada and does not contribute to strengthening our economy.

Canada will lead by industrializing AI at home, by driving adoption at scale across our economy, and that is where sovereignty becomes real. We will lead by industrializing AI, by driving adoption at scale across our economy. That is the railroad moment for Canada. In the past, we built infrastructure that connected the country and unblocked growth. Today, we must build digital infrastructure for AI that does the same. We must build a sovereign AI capability that businesses and institutions can tap into easily, reliably and at scale.

To do this, we can rely on global technologies in some areas, but they must operate within Canadian-controlled infrastructure and governance. That means our networks must be sovereign, our data must be governed here with control over how it moves and where it is processed, our data centres must be powered by Canadian energy, and we must have authority over the compute infrastructure that powers AI workloads. That is the digital equivalent of owning the rails.

On top of those rails, we must enable what matters most: adoption at scale. That means technologies that connect AI to real data, workflows and decisions inside Canadian enterprises and institutions. This is because today Canada has a structural problem. We are exceptional at the science behind AI, but we have not adopted AI meaningfully at home, and we have not consistently monetized it globally. If we stay on this path, we will lose control over our data, our infrastructure and the economic value created by AI systems.

The alternative is clear: Canada must move from being a research leader to also becoming an industrialization leader for AI anchored in sovereignty. In practical terms, that means two

Canada n'en tirera aucune valeur économique et ne renforcera pas non plus sa position en essayant de dépenser plus que les autres à cet égard.

Cela dit, le Canada doit absolument continuer à investir dans la recherche. Nous disposons de talents de calibre mondial et nous avons contribué de manière importante aux progrès mondiaux en matière d'IA.

Cependant, il arrive trop souvent que ces talents ne soient pas mis à profit ici, au Canada, au service de notre pays, et qu'ils ne contribuent pas à renforcer notre économie.

Le Canada jouera un rôle de premier plan en favorisant l'industrialisation de l'IA sur son territoire et son adoption à grande échelle dans l'ensemble de notre économie. C'est dans ce contexte que la souveraineté prend tout son sens. Nous jouerons un rôle de premier plan en industrialisant l'IA et en favorisant son adoption à grande échelle dans l'ensemble de notre économie. C'est pour le Canada l'occasion d'une nouvelle ère, comparable à celle de l'avènement du chemin de fer. Par le passé, nous avons construit des infrastructures qui ont permis de relier les différentes régions du pays et de favoriser la croissance. Aujourd'hui, nous devons construire des infrastructures numériques qui feront la même chose pour l'IA. Nous devons mettre en place une capacité souveraine en matière d'IA à laquelle les entreprises et les institutions pourront avoir accès facilement, de manière fiable et à grande échelle.

Pour ce faire, nous pouvons nous appuyer sur des technologies utilisées mondialement dans certains domaines, mais celles-ci doivent fonctionner au sein d'une infrastructure et d'une gouvernance contrôlées par le Canada. Cela signifie que nos réseaux doivent être souverains, que nos données doivent être gérées ici, qu'un contrôle doit s'exercer sur la circulation de ces données et sur les endroits où elles sont traitées et que nos centres de données doivent être alimentés par de l'énergie canadienne. Nous devons aussi avoir autorité sur l'infrastructure informatique qui alimente les charges de travail de l'IA. C'est l'équivalent numérique du fait d'être propriétaire des rails.

Sur ces rails, nous devons rendre possible ce qui compte le plus : l'adoption à grande échelle. Cela signifie qu'il nous faut des technologies qui relient l'IA aux données réelles, aux flux de travail et aux décisions au sein des entreprises et des institutions canadiennes. Or, le Canada se bute présentement à un problème d'ordre structurel. Nous excellons dans la science qui sous-tend l'IA, mais nous n'avons pas adopté l'IA de manière significative chez nous, et nous ne l'avons pas systématiquement monétisée à l'échelle mondiale. Si nous continuons sur cette voie, nous perdrons le contrôle de nos données, de notre infrastructure et de la valeur économique que créent les systèmes d'IA.

L'alternative est sans équivoque : le Canada doit passer du statut de meneur dans le domaine de la recherche à celui de meneur dans celui de l'industrialisation de l'IA, ancré dans la

things: First, it means building a sovereign AI stack that Canadian organizations can tap into — a fully operational, accessible infrastructure, spanning data, compute and applications, governed under Canadian authority. Second, and most critically, it means accelerating enterprise adoption at scale.

Today, too many organizations remain stuck in experimentation mode, while global competitors are already operating AI in production. This gap is already visible in productivity, cost structures and speed of innovation. If Canadian enterprises and institutions do not embed AI into their core operations, they will compete at a structural disadvantage.

Government has a critical role to play here: To act as a demand engine through procurement, incentivizing deployment and not just research, and reducing friction through clear, consistent regulatory frameworks.

The Chair: Your five minutes are up, but we are sure to get the rest of your points during our question period.

Ms. Dassa: Okay. Thank you.

The Chair: Thank you. We will now hear from Mr. Menezes.

John Menezes, President and Chief Executive Officer, Bell Cyber Inc., Bell Canada: Good morning, chair and honourable senators.

Thank you for the opportunity to be here today. As a first-generation immigrant to Canada, this moment is deeply meaningful to me. To be invited to contribute to a national conversation of this importance in a country that has given me so much is something I do not take lightly.

Canada is at an inflection point. Artificial intelligence is rapidly moving from research into the core of our economy, reshaping how we operate, how we compete and how we deliver services. The question before us is not whether AI will transform Canada; it is whether Canada will shape that transformation or allow it to be shaped elsewhere.

I would add that AI is moving faster than our ability to govern it, and that gap is where the risk lives. The scale of change is significant. Tens of millions of jobs will be reshaped every year

souveraineté. Concrètement, cela signifie deux choses : premièrement, il s'agit de construire une infrastructure souveraine en matière d'IA à laquelle les organisations canadiennes peuvent avoir accès — une infrastructure sous autorité canadienne pleinement opérationnelle et accessible, couvrant les données, la puissance de calcul et les applications. Deuxièmement, et c'est le plus crucial, cela signifie qu'il faut accélérer l'adoption à grande échelle de l'IA par les entreprises.

Aujourd'hui, trop d'organisations restent bloquées en mode expérimental, tandis que leurs concurrents mondiaux exploitent déjà l'IA dans un contexte de production. Cet écart se manifeste déjà sur le plan de la productivité, des structures de coûts et de la vitesse d'innovation. Si les entreprises et les institutions canadiennes n'intègrent pas l'IA dans leurs opérations de base, elles seront confrontées à un désavantage structurel face à la concurrence.

Le gouvernement a un rôle crucial à jouer ici : agir comme un moteur de la demande par le biais des marchés publics, en encourageant le déploiement et pas seulement la recherche, et en réduisant les frictions grâce à des cadres réglementaires clairs et cohérents.

La présidente : Vos cinq minutes sont écoulées, mais il ne fait aucun doute que nous entendrons le reste de votre argumentaire lors de la période des questions.

Mme Dassa : D'accord. Merci.

La présidente : Merci. Nous allons maintenant entendre M. Menezes.

John Menezes, président et chef de la direction, Bell Cyber Inc., Bell Canada : Madame la présidente, honorables sénateurs, bonjour.

Merci de m'avoir donné la chance d'être ici aujourd'hui. En tant qu'immigrant de première génération au Canada, ce moment revêt une grande importance pour moi. Être invité à contribuer à un débat national de cette importance dans un pays qui m'a tant donné est quelque chose que je ne prends pas à la légère.

Le Canada se trouve à un moment décisif de son histoire. L'intelligence artificielle est en train de passer rapidement du stade de la recherche à celui d'occuper une place centrale dans notre économie. Elle est en train de restructurer nos façons de faire, de rivaliser et de fournir des services. La question qui se pose n'est pas de savoir si l'IA va transformer le Canada, mais si le Canada va façonner cette transformation lui-même ou la laisser se façonner ailleurs.

J'ajouterais que l'IA évolue plus vite que notre capacité à la réguler, et que c'est dans cet écart que réside le risque. L'ampleur du changement est considérable. Des dizaines de

by AI — not eliminated, but fundamentally redesigned. Within just a few years, virtually every knowledge worker will be impacted.

This is not incremental change. This is a complete redefinition of how work gets done. At Bell, we see this transformation across the full value chain: from infrastructure to AI adoption to security.

My colleague Michel Richer can provide more detail about how we are investing in sovereign AI infrastructure, ensuring that Canadian data, compute and capabilities remain under Canadian control.

That is because sovereignty in AI is not theoretical; it is operational. It depends on where data resides, who controls the compute, how systems are connected and who ultimately has authority over them.

My role is to focus on what makes all of that possible: trust. That starts with cybersecurity. There is no AI strategy without a cybersecurity strategy. Without it, there is no trust, and without trust, there is no adoption.

AI systems depend on data, make decisions and, increasingly, act autonomously. That introduces entirely new categories of risk. We are already seeing examples of AI systems that are considered too powerful or too unpredictable to be broadly released. That is not a future concern; that is happening now. That means security must evolve at the same pace as capability.

At Bell Cyber, we are not just talking about this; we are living it. We recently launched North America's first autonomous security operations centre. When we did, I had a very direct conversation with my team. I told them this:

> The jobs you are doing today will not exist in their current form within a year, not because you are not needed, but because you are needed at a higher level.

That is the reality of AI. It is already better at processing massive volumes of data, detecting patterns and responding to threats in real time. So the role of human beings must evolve from reacting to advising and from executing to guiding.

millions d'emplois seront remodelés chaque année par l'IA — non pas supprimés, mais fondamentalement repensés. D'ici quelques années à peine, pratiquement tous les travailleurs du savoir seront touchés.

Il ne s'agit pas d'un changement progressif. Il s'agit plutôt d'une redéfinition complète de nos façons de travailler. Chez Bell, nous observons cette transformation tout au long de la chaîne de valeur : de l'infrastructure à l'adoption de l'IA, en passant par la sécurité.

Mon collègue Michel Richer peut vous fournir plus de détails sur la façon dont nous investissons dans une infrastructure d'IA souveraine qui nous permettra d'assurer que les données, la puissance de calcul et les capacités canadiennes restent sous contrôle canadien.

En effet, la souveraineté en matière d'IA n'est pas une question théorique, mais bien opérationnelle. Elle dépend de l'emplacement des données, de l'identité de ceux qui contrôlent la puissance de calcul, de la manière dont les systèmes sont connectés et de qui, en fin de compte, la commandent.

Mon rôle consiste à me concentrer sur ce qui rend tout cela possible : la confiance. Et cela commence par la cybersécurité. Il n'y a pas de stratégie en matière d'IA sans stratégie concernant la cybersécurité. Sans cela, il n'y a pas de confiance, et sans confiance, il n'y a pas d'adoption.

Les systèmes d'IA dépendent des données. Ils prennent des décisions et agissent de plus en plus de manière autonome. Cela crée des catégories de risques complètement nouvelles. Nous voyons déjà des exemples de systèmes d'IA que l'on juge trop puissants ou trop imprévisibles pour être déployés à grande échelle. Ce n'est pas une préoccupation sur ce qui pourrait arriver, mais sur ce qui se produit présentement. Conséquemment, la sécurité doit évoluer au même rythme que les capacités.

Chez Bell Cyber, nous ne nous contentons pas d'en parler : nous le vivons. Nous avons récemment lancé le premier centre d'opérations de sécurité autonome d'Amérique du Nord. À cette occasion, j'ai eu une conversation très franche avec les membres de mon équipe, et voici ce que je leur ai dit :

> D'ici un an, les emplois que vous occupez n'existeront plus dans leur forme actuelle. Ce n'est pas parce que nous n'aurons plus besoin de vous, mais bien parce que vos services sont requis à un niveau supérieur.

Telle est la réalité de l'IA. Déjà, elle arrive mieux que nous à traiter d'énormes volumes de données, à dégager des profils et à répondre aux menaces en temps réel. Le rôle des êtres humains doit donc évoluer : passer de la réaction à la prestation de conseils, et de l'exécution à l'encadrement.

At Bell Cyber, we're not preparing for this shift; we're already operating in it.

Government has a critical role to play. But AI does not evolve in predictable cycles. It evolves continuously. That challenges traditional approaches to policy and regulation. We cannot rely solely on fixed, long-term frameworks for a technology that is changing in real time, which is why collaboration is so essential.

The private sector is where AI is being built and deployed, and where risks are first encountered. Government brings direction, trust and the ability to scale impact nationally. Bringing these together is not optional; it is necessary.

I'll close with this: If Canada wants to lead in AI, we must lead in trusted AI, and that starts with security, sovereignty and the ability to act at scale. The opportunity is real, but it is time bound. The transformation is already under way. The decisions we make now will determine whether Canada leads or follows.

At Bell, across Bell AI Fabric and Bell Cyber, we are committed to helping Canada lead.

Thank you. We look forward to your questions.

The Chair: Thank you, Mr. Menezes. We will now proceed to questions from committee members. For this panel, senators we will have four minutes for their question, which also includes the answer.

Senator Burey: Thank you so much for being here today. These are very deep, existential questions that we have to try to wrap our minds around today.

From our first witness. I heard that, with the frontier models, we will not have enough funds to do it, so we should stick to industrialization AI for Canada, which is analogous to the railroad.

Next, I heard from you, Mr. Menezes, that we must lead in trust and cybersecurity. If we don't have our foot in the frontier models, how are we going to lead in trust and cybersecurity?

Mr. Menezes: They are not mutually exclusive. No matter where the models are developed, you still have to secure them. When you implement a model, whether it is a frontier model or

Chez Bell Cyber, nous ne sommes pas en train de nous préparer à cette transition; nous y sommes déjà.

Le gouvernement a un rôle crucial à jouer à cet égard, toutefois, l'IA n'évolue pas selon des cycles prévisibles. Elle évolue en continu, ce qui entraîne une remise en question des approches traditionnelles en matière de politique et de réglementation. Avec une technologie qui change en temps réel, nous ne pouvons pas nous fier uniquement à des cadres fixes et à long terme, et c'est pourquoi la collaboration est à ce point essentielle.

C'est dans le secteur privé que l'IA est développée et déployée, et que les risques se manifestent en premier lieu. Le gouvernement donne une orientation, consolide la confiance et apporte la capacité d'amplifier l'impact à l'échelle nationale. La réunion de ces éléments n'est pas facultative, mais bien nécessaire.

Je terminerai par ceci : si le Canada veut être un chef de file en matière d'IA, il doit l'être dans le domaine de l'IA de confiance, et cela commence par la sécurité, la souveraineté et la capacité d'agir à grande échelle. L'opportunité est réelle, mais elle est limitée dans le temps. La transformation est déjà en cours. Les décisions que nous prenons aujourd'hui détermineront si le Canada sera un meneur ou un suiveur.

Chez Bell — par l'intermédiaire du Réseau d'IA tissé de Bell et Bell Cyber —, nous nous engageons à aider le Canada à jouer un rôle de premier plan.

Merci. Nous serons plus qu'heureux de répondre à vos questions.

La présidente : Merci, monsieur Menezes. Nous allons maintenant passer aux questions des membres du comité. Pour ce groupe d'experts, les sénateurs disposeront de quatre minutes pour poser leur question, réponse incluse.

La sénatrice Burey : Merci beaucoup d'être ici aujourd'hui. Les questions dont nous sommes saisis aujourd'hui sont des questions très profondes et existentielles.

À notre premier témoin, vous nous avez dit que le Canada n'avait pas les ressources suffisantes pour s'attaquer aux modèles de pointe, et qu'il devait plutôt s'en tenir à l'industrialisation de l'IA à l'échelle du pays, ce qui a été comparé à la construction du chemin de fer.

Ensuite, j'ai entendu de votre bouche, monsieur Menezes, que nous devons être à l'avant-garde en matière de confiance et de cybersécurité. Si nous ne nous engageons pas du côté des modèles de pointe, comment allons-nous nous retrouver à l'avant-garde en matière de confiance et de cybersécurité?

M. Menezes : Ces deux aspects ne s'excluent pas mutuellement. Peu importe où les modèles sont développés, il faut toujours les sécuriser. Lorsque vous mettez en œuvre un

any other kind of model, you still have to put the guardrails in place; you have to make sure that the AI is going to do what you want it to do and that it behaves properly. Security is a fundamental part of it. No matter which model you have, and where the model is developed, when it is implemented in Canada, it has to be implemented with the guardrails necessary to ensure that it is doing what we think it should be doing.

Senator Burey: Can you comment on the guardrails?

Mr. Menezes: The guardrails are very simple. When a child asks a question, we want to make sure that the AI is giving an answer that is applicable to a child. When AI is being asked a question, we want to make sure that the answer is not toxic. We want to make sure the answer is not biased. We want to make sure that the answer is not racist. So those are simple guardrails. If someone decides, I want to know how to build an improvised explosive device, or IED, we want to ensure that the AI does not give that answer. Rather, the AI says, I'm not permitted to give you that answer. That's what we mean by putting in guardrails: It is to control the AI.

Senator Burey: Ms. Dassa, do you have any comments?

Ms. Dassa: Yes. I agree completely with the previous comments. I would add that the goal is strategic control over what matters most: data, critical work loads and governance. My allusion to sovereignty is that it is not only about the data flowing through the system; it is about which legal jurisdiction governs the provider managing that data. We can remain globally connected while ensuring that critical capabilities around governance and safety operate under Canadian control. That's sovereignty without isolation.

Senator Burey: Thank you.

Senator Hay: Thank you all for being here. We appreciate it.

I will ask something of you first, Mr. Menezes. When you first stepped into the foray of cyber, that was 25 plus years ago. It was something to worry about, but it is now so radically different. I want you to speak about speed because, as we were speaking about, and as Janice Stein was speaking about earlier this week, what was going on three months ago has already changed. I'm curious about your approach to that. How do you stay at speed when it comes to trust?

modèle, qu'il s'agisse d'un modèle de frontière ou de tout autre type de modèle, vous devez toujours mettre en place des garde-fous. Vous devez vous assurer que l'intelligence artificielle fera ce que vous attendez d'elle et qu'elle se comportera correctement. La sécurité est un élément fondamental de cela. Quel que soit le modèle dont vous disposez et quel que soit le lieu où il est développé, lorsqu'il est mis en œuvre au Canada, il doit l'être avec les garde-fous nécessaires pour garantir qu'il fait ce que nous pensons qu'il devrait faire.

La sénatrice Burey : Pouvez-vous nous en dire plus sur ces garde-fous?

M. Menezes : Les garde-fous sont très simples. Lorsqu'un enfant pose une question, nous voulons nous assurer que l'intelligence artificielle donne une réponse adaptée à un enfant. Lorsqu'une question est posée à l'intelligence artificielle, nous voulons nous assurer que la réponse n'est pas toxique. Nous voulons nous assurer que la réponse n'est pas biaisée. Nous voulons nous assurer que la réponse n'est pas raciste. Ce sont donc des garde-fous simples. Si quelqu'un décide qu'il veut savoir comment fabriquer un engin explosif improvisé, nous voulons nous assurer que l'intelligence artificielle ne lui dise pas comment faire. Au contraire, l'intelligence artificielle devrait répondre : « Je ne suis pas autorisée à vous donner cette réponse. » C'est ce que nous entendons par « mettre en place des garde-fous » : il s'agit de contrôler l'intelligence artificielle.

La sénatrice Burey : Madame Dassa, souhaitez-vous intervenir?

Mme Dassa : Oui. Je suis tout à fait d'accord avec ces observations. J'ajouterais que l'objectif est d'exercer un contrôle stratégique sur ce qui importe le plus, c'est-à-dire les données, les charges de travail critiques et la gouvernance. Lorsque j'évoque la souveraineté, je ne parle pas seulement des données qui transitent par le système. Il s'agit aussi de savoir quelle administration régit le fournisseur qui gère ces données. Nous pouvons rester connectés au monde tout en veillant à ce que les capacités névralgiques en matière de gouvernance et de sécurité opèrent sous contrôle canadien. C'est ce que signifie la souveraineté sans l'isolement.

La sénatrice Burey : Je vous remercie.

La sénatrice Hay : Merci à tous de votre présence parmi nous. Vous avez toute notre reconnaissance.

Je vais d'abord m'adresser à vous, monsieur Menezes. Lorsque vous vous êtes lancé dans le domaine de la cybernétique, c'était il y a plus de 25 ans. C'était un sujet de préoccupation, mais la situation est aujourd'hui radicalement différente. Je voudrais que vous nous parliez de la rapidité, car, comme nous en discutions et comme Janice Stein l'a mentionné plus tôt cette semaine, ce qui se passait il y a trois mois a déjà changé. Je suis curieux de connaître votre approche à ce sujet.

Comment faites-vous pour rester à la page en matière de confiance?

For my final question, Janice Stein also said that it is not so much about control of our sovereignty; it is about being free from coercion. I am just curious about speed, staying up with it, cyber and coercion versus control.

Pour ma dernière question, Janice Stein a également déclaré qu'il ne s'agissait pas tant de contrôler notre souveraineté que d'être à l'abri de toute coercition. Je suis simplement curieux de savoir comment vous gérez la rapidité, comment vous suivez le rythme, et comment vous conciliez cyberespace et coercition avec la notion de contrôle.

Mr. Menezes: I have been in cybersecurity now since 1992. So that is about 34 years in cybersecurity. I have been running a managed security services company for 25 years. We are protecting customers across the world. I was never afraid of being in the security business because I always thought we were very secure. Then, two years ago, AI started to appear, and as I was telling my team just a few months ago, for the first time in my career, I don't sleep well at night because I'm concerned about the protection of my customers.

M. Menezes : Je travaille dans le domaine de la cybersécurité depuis 1992, soit environ 34 ans. Je dirige une entreprise de services de sécurité gérés depuis 25 ans. Nous protégeons des clients partout dans le monde. Je n'ai jamais eu peur de travailler dans le secteur de la sécurité, car j'ai toujours pensé que nous offrions une très bonne protection. Puis, il y a deux ans, l'intelligence artificielle a commencé à faire son apparition. Comme je l'ai dit à mon équipe il y a quelques mois à peine, je dors mal la nuit pour la première fois de ma carrière, parce que je m'inquiète au sujet de la protection de mes clients.

AI has fundamentally changed everything. What is happening now is that we do not know how the AI is going to behave. Even though we are talking about all these different models and the frontier models, nobody really knows how the AI is going to work. Nobody knows how the AI is going to behave. We're learning everything, and we're learning at speed.

L'intelligence artificielle a tout changé de manière fondamentale. Le fait est que nous ne savons pas comment elle va se comporter. Nous avons beau parler de tous les différents modèles, y compris les plus avancés, personne ne sait vraiment comment l'intelligence artificielle va fonctionner. Personne ne sait comment elle va se comporter. Nous avons tout à apprendre, et nous l'apprenons à grande vitesse.

Sometimes when governments talk, we talk about a three-year plan or a five-year plan. Somebody said to me, "What is your two-year plan for AI," and I said, "I have a two-month plan for AI." It is moving so fast.

Les gouvernements parlent parfois de plans triennaux ou quinquennaux. Quelqu'un m'a demandé quel était mon plan sur deux ans pour l'intelligence artificielle. Je lui ai répondu : « J'ai un plan sur deux mois pour l'IA. » Les choses évoluent tellement vite.

What is happening is that industry and businesses are looking at AI as a perfect way to reduce costs and cut down the number of jobs and people working. They are moving rapidly. We cannot secure AI, but we have got to move rapidly because the business is demanding it. So everybody is asking the questions, "How can I use AI to make my job or business more efficient? How can I increase my profits?" So there is speed at both sides. On the business side, everybody is racing forward, and on the AI side, everybody is racing forward.

Concrètement, l'industrie et les entreprises voient dans l'intelligence artificielle un moyen idéal de réduire les coûts et de diminuer le nombre d'emplois et de salariés. Elles vont rapidement de l'avant. Nous ne pouvons pas sécuriser l'intelligence artificielle, mais nous devons passer aux actes rapidement, car les entreprises l'exigent. Tout le monde se demande : « Comment puis-je utiliser l'IA pour améliorer mon efficacité au travail ou celle de mon entreprise? Comment puis-je augmenter mes profits? » Tant du côté des entreprises que de celui de l'intelligence artificielle, tout le monde a le pied sur l'accélérateur et fonce droit devant.

You see OpenAI and Elon Musk, and they are all arguing about who can have the better model moving forward. The change has been so dramatic — so dramatic — even in the last three months. For instance, in my own personal life, I can prepare a presentation in three minutes. A PowerPoint presentation that would take my marketing team two weeks to do for me can now be prepared in three minutes, and it is a better presentation than my marketing team could develop in two weeks. As a businessperson, should I reduce the number of people on my marketing team?

On voit OpenAI et Elon Musk, et personne ne s'entend sur qui aura le meilleur modèle à l'avenir. Le changement a été tellement fulgurant — vraiment fulgurant —, même au cours des trois derniers mois. En voici un exemple personnel: je peux préparer une présentation en trois minutes. Une présentation PowerPoint qui prendrait deux semaines à mon équipe marketing peut désormais être préparée en trois minutes, et elle est meilleure que celle que mon équipe marketing pourrait élaborer en deux semaines. En tant qu'entrepreneur, devrais-je réduire les effectifs de mon équipe marketing?

Senator Hay: Thank you.

Senator Senior: Mr. Menezes, what you said troubled me. For someone who has been in cybersecurity for such a long time, the fact that you are having sleepless nights, yet you are saying that trust is critical. I don't know how those two things go together. As we are trying to figure out the path that we're going to take and what we're going to recommend coming out of this study, if someone with such depth of experience and knowledge is not sleeping at night, then I won't sleep at night, and many Canadians won't either.

Ms. Dassa referred to the importance of governance, and that the importance of Canadian frontier building is not the main element; rather, it is about how we govern. I think you also talked about that. It is to ensure that we can control AI. Is it controllable if it is going so fast?

Mr. Menezes: I don't believe so. We can talk about guardrails, but everybody is building very sophisticated models, and nobody really knows — not the builders, not the users — how the AI is going to go.

When the Anthropic CEO said the other day, "I think my AI is conscious." We don't know. We really do not know. We have theories. We can put guardrails, but we don't know.

As a cybersecurity expert, we have been trying for the last two years to figure out how we control it. But you go down one path, and then everything changes very quickly. Then you have to go down another path, and then everything changes very quickly. I have a six-month project plan, and we're going to phase one, then phase two and then phase three. With AI security, you start phase one, and then it changes; then you start phase two, and then it changes; then you come back to phase one.

To be honest with you, it is a frightening time in our world with AI. It is absolutely frightening. I love using AI, and everybody uses ChatGPT to write their emails and so forth. But that's not where the challenge is. The challenge is with AI agents. For every one human identity, there are going to be 200 agent identities. It is going to be a nightmare. It is going to be a nightmare for how you control all these agents that are running around and doing things on their own.

Senator Senior: Ms. Dassa, do you agree? If not, why not?

La sénatrice Hay : Merci.

La sénatrice Senior : M. Menezes, vos propos m'ont troublée. Vous travaillez dans le domaine de la cybersécurité depuis très longtemps, mais vous passez des nuits blanches. Pourtant, vous affirmez que la confiance est essentielle. Je ne vois pas comment ces deux choses peuvent être réconciliables. Nous essayons de déterminer la voie à suivre et les recommandations à formuler à l'issue de cette étude. Or si une personne dotée d'une telle expérience et d'une telle expertise ne dort pas la nuit, moi non plus je ne dormirai pas ni de nombreux Canadiens d'ailleurs.

Mme Dassa a souligné l'importance de la gouvernance, en précisant que ce n'est pas tant le perfectionnement au Canada qui importe, mais la manière dont nous gouvernons. Je crois que vous en avez également parlé. Nous devons avoir la capacité de contrôler l'intelligence artificielle. Peut-on la contrôler alors qu'elle évolue à un rythme aussi effréné ?

M. Menezes : Je ne pense pas. On peut bien parler de garde-fous, mais tout le monde élabore des modèles très sophistiqués, et personne ne sait vraiment — ni ceux qui les développent ni ceux qui les utilisent — comment l'intelligence artificielle évoluera.

Le PDG d'Anthropic a déclaré l'autre jour qu'il pense que son intelligence artificielle est consciente. Nous n'en savons rien. Nous n'en savons littéralement rien. Nous avons des théories. Nous pouvons mettre en place des garde-fous, mais nous n'en savons rien.

Nous sommes des experts en cybersécurité. Nous cherchons depuis deux ans des moyens de contrôler l'intelligence artificielle. Malheureusement, nous prenons une voie, puis tout change très vite. Il faut alors emprunter une autre voie, et là encore, tout change très vite. J'ai un plan de projet sur six mois. Nous passons à la première phase, puis à la deuxième, puis à la troisième. Avec la sécurité de l'IA, on commence la première phase, puis ça change; ensuite, on commence la deuxième phase, puis ça change, puis on revient à la première phase.

Si je suis franc avec vous, je dirais que nous vivons une époque terrifiante à cause de l'intelligence artificielle. C'est vraiment terrifiant. J'adore utiliser l'intelligence artificielle. Tout le monde utilise ChatGPT pour rédiger ses courriels et ainsi de suite. Toutefois, ce n'est pas là le problème. Le problème, ce sont les agents d'intelligence artificielle. Pour chaque identité humaine, il y aura 200 identités d'agents. Ce sera un cauchemar. Trouver le moyen de contrôler tous ces agents qui circulent partout et agissent de leur propre chef sera un cauchemar.

La sénatrice Senior : Mme Dassa, êtes-vous du même avis? Sinon, pourquoi?

Ms. Dassa: I believe the solution is not to slow adoption but to structure it properly: strong data governance, clear accountability for AI decisions and human oversight in critical workflows. Those are three practical layers, where safety comes from how AI is deployed and not just how it is built: models operated on trusted control data, the ability to trace decisions and output; and connecting AI to enterprise or institutional data as opposed to relying on only generic models. That is how we can build safety and trustworthiness in how we deploy applied AI.

Mme Dassa : Selon moi, la solution n'est pas de freiner l'adoption de l'intelligence artificielle, mais de l'encadrer correctement en assurant une gouvernance rigoureuse des données, une reddition de comptes claire à l'égard des décisions prises par l'intelligence artificielle et une surveillance humaine dans les flux de travail critiques. Ce sont là trois niveaux où la sécurité dépend concrètement de la manière dont l'intelligence artificielle est déployée, et non seulement de la façon dont elle est conçue. Il s'agit de modèles utilisant des données de contrôle fiables, offrant la possibilité de retracer les décisions et leurs résultats et connectant l'intelligence artificielle aux données de l'entreprise ou de l'institution au lieu d'utiliser uniquement des modèles génériques. Voilà comment nous pouvons déployer l'intelligence artificielle appliquée de manière fiable et sécuritaire.

The Chair: Thank you.

La présidente : Merci.

Senator Cardozo: My question is for John Menezes. Let me first say, as full disclosure, some of you will recall that I gave a speech on the contribution of immigrants recently in the chamber, and one of the people I highlighted was Mr. Menezes. So now you can prove whether I was right or not to highlight your contribution.

Le sénateur Cardozo : Ma question s'adresse à John Menezes. Je précise, par souci de transparence, que j'ai récemment prononcé un discours au Sénat sur la contribution des immigrants, certains parmi vous s'en souviendront peut-être. M. Menezes est l'une des personnes que j'ai mentionnées. Le moment est venu de montrer si j'ai eu raison ou non de souligner votre apport.

I have two questions. You talked about where data resides. All our data and all our systems seem to reside in the U.S. Can the American President call his tech bros and tell them to cut the internet off in Canada if he gets upset at us? That's number one.

J'ai deux questions. Vous avez parlé de l'emplacement des données. Toutes nos données et tous nos systèmes semblent se trouver aux États-Unis. Le président des États-Unis peut-il appeler ses acolytes du secteur des technologies et leur demander de couper Internet au Canada s'il en a contre nous? Voilà pour la première question.

Mr. Menezes: A quick one, yes.

M. Menezes : En un mot, oui.

Senator Cardozo: Okay. I don't know if I should say thank you, but thank you for the answer.

Le sénateur Cardozo : D'accord. Je ne sais pas si je dois dire merci, mais je vous remercie de votre réponse.

In terms of AI and the security systems that you have created, I think of *2001: A Space Odyssey*, the movie, where the computer became mad at the humans. Can that happen? Let's say you have set up a confidential system of information. Can the computer, an AI, decide to release all the information you have secured for your clients and decide, no, that shouldn't be confidential, and it is going to put it out to the world?

Prenons l'intelligence artificielle et les systèmes de sécurité que vous avez mis au point et pensons au film *2001 : L'Odyssée de l'espace*, dans lequel l'ordinateur se retourne contre les humains. Est-ce que cela pourrait arriver? Imaginons que vous ayez mis en place un système d'informations confidentielles. L'ordinateur, en tant qu'IA, pourrait-il décider de divulguer toutes les informations que vous avez protégées pour vos clients parce qu'il estime que celles-ci ne devraient pas être confidentielles, mais qu'elles devraient être rendues publiques?

Mr. Menezes: The risk is there, absolutely. The risk is there that the AI can lose its mind and do things on its own.

M. Menezes : Le risque existe bel et bien. Il y a un risque que l'intelligence artificielle perde le nord et agisse de son propre chef.

There was an example just a few months ago with a tech CEO whose emails were being deleted, and even when she told the AI to stop deleting the emails, it kept on deleting the emails and

Il y a quelques mois à peine, on a vu le cas d'une PDG d'une entreprise technologique dont les courriels étaient supprimés. Même après qu'elle a demandé à l'intelligence artificielle

said, “Oh, you know, I made a mistake.” So the AI can do actions like that.

The challenge that we are having, as Alex said, is that we have to govern the AI. We have to have all the traceability. But it is all so new. What we are talking about is theoretical because these models have just been developed. We are just trying to figure out how the AI is doing things, and there is a lot of learning that has to happen to figure out how we can control the AI and how we can make sure that the AI does not go off and do its own thing.

We are very much in the infancy stage of AI, and at the infancy stage, we are having problems.

Senator Cardozo: If we are at the infancy stage, any guardrails we put in, can’t AI just get rid of them and get over them and dismiss them? Is there anything we can do?

Mr. Menezes: Again, we don’t know the answer to that. We have theoretical answers. Yes, you put the guardrails in, and the AI is going to behave, but we have seen cases where the guardrails haven’t taken effect or haven’t done what they are supposed to do. We think we are going to see many more cases where the AI goes rogue on us.

Senator Cardozo: I’m sorry to go down this path, which is darker and darker, but can AI decide to go to war? For example, we have jets flying over. Can AI just stop them, drop them out of the sky or stop their abilities to defend us or whatever?

Mr. Menezes: If you have noticed, in the last month, Anthropic, which is the creator of Claude, was having a lot of problems with the U.S. Department of Defense because the U.S. Department of Defense wanted Anthropic to give them the LLMs without the guardrails. Anthropic said, we are not going to do that because if we give you the LLMs without guardrails, you can go and do everything that you suggested just now.

So there’s a bit of push and pull going on between the creators of the LLMs and government agencies. It’s not just in North America; it’s the Chinese, the Russians and everyone else. They are all busy developing LLMs and developing these frontier models. Are they going to have guardrails like we have? If we put guardrails, are we tying our hand behind our back?

d’arrêter, cette dernière a continué de le faire en disant : « Oh, vous savez, j’ai fait une erreur. » L’intelligence artificielle est donc capable d’agir de la sorte.

La difficulté à laquelle nous sommes confrontés, comme l’a dit Mme Dassa, c’est qu’il faut réguler l’intelligence artificielle. Il faut une parfaite traçabilité. Or, tout cela est tellement nouveau. Ce dont nous parlons est théorique, car ces modèles viennent tout juste d’être conçus. Nous cherchons simplement à comprendre comment l’intelligence artificielle se comporte. Nous avons encore beaucoup à apprendre pour déterminer comment la contrôler et nous assurer qu’elle ne se met pas à agir de son propre chef.

Nous n’en sommes qu’aux premiers pas de l’intelligence artificielle, et à ce stade, nous sommes confrontés à des difficultés.

Le sénateur Cardozo : Si nous n’en sommes qu’aux premiers pas, l’intelligence artificielle ne risque-t-elle pas de contourner, de passer outre et d’ignorer tous les garde-fous que nous mettons en place? Y a-t-il quelque chose que nous pouvons faire?

M. Menezes : Encore une fois, nous ne connaissons pas la réponse à cette question. Nous avons des réponses théoriques. Certes, si l’on met en place des garde-fous, l’intelligence artificielle se comportera correctement, mais il y a déjà eu des cas où ces garde-fous n’ont pas fonctionné ou n’ont pas rempli leur rôle. Nous sommes d’avis que nous verrons de nombreux autres cas où l’intelligence artificielle nous jouera des tours.

Le sénateur Cardozo : Je suis désolé de poursuivre sur cette voie, qui devient de plus en plus sombre, mais l’intelligence artificielle peut-elle décider de déclencher une guerre? Par exemple, si des avions de chasse survolent notre territoire, l’intelligence artificielle peut-elle simplement les arrêter, les faire tomber ou les empêcher de nous défendre, ou toute autre chose du genre?

M. Menezes : Vous avez peut-être eu vent que le mois dernier, Anthropic, la société qui a créé Claude, a eu de nombreux problèmes avec le ministère états-unien de la Défense. Ce dernier souhaitait qu’Anthropic lui fournisse les grands modèles de langage sans mécanismes de contrôle. Anthropic a répondu qu’elle ne le ferait pas, car si elle lui fournissait ces modèles sans ces mécanismes, tout ce que vous venez de dire pourrait se réaliser.

On assiste donc à une sorte de bras de fer entre les créateurs de ces grands modèles de langage et les organismes gouvernementaux. Cela ne se passe pas qu’en Amérique du Nord : c’est aussi le cas en Chine, en Russie et partout ailleurs. Tout le monde s’affaire à développer ces grands modèles de langage et ces modèles avancés. Mettront-ils en place des garde-fous comme nous l’avons fait? En mettant en place des garde-fous, sommes-nous en train de nous pénaliser?

Senator Boudreau: I have one quick question for Ms. Dassa and one quick question for Mr. Menezes.

Ms. Dassa, you said, in your opening remarks, that basically data sovereignty is imperative — if I paraphrase — and you put a lot of emphasis on that. But we've heard that the U.S. CLOUD Act basically prevents this from happening, 100%, because already the U.S. government — and my colleague just talked about that — can compel other countries to turn over their data. How do you respond to that? Is data sovereignty possible with the CLOUD Act?

Ms. Dassa: In short, yes. What matters is not just where the data is located, but which legal system governs the proprietor managing or accessing that data.

In certain cases, if a service provider is headquartered or legally subject to a foreign jurisdiction, that jurisdiction may have laws that allow authorities to request data held or controlled by that provider. That all depends on how the service is structured.

So it comes back to how we adopt applied AI in a safe, trustworthy way that is governed properly. So sovereignty — in the way that it is possible — focuses on who controls the infrastructure, under which laws that infrastructure operates, which is why it is so incredibly important that the data flows through networks that are on Canadian soil and where the compute is governed, managed and controlled, and which courts have authority over those access requests.

So the three elements that matter are not so much the engagement layer, but really the governance layer. Networks need to be sovereign — we have those; our data has to be governed here with control over how it moves and where it's processed; and our data centres need to be powered by Canadian energy as well so that we have authority throughout, as well as over the compute infrastructure that powers AI workloads, which is possible and feasible.

We have those resources here in Canada, but it doesn't mean that it is not possible to also act as a good global citizen and engage with other global technology providers, as long as we have control over those elements and those layers, which is entirely feasible.

Senator Boudreau: Mr. Menezes, you started off by basically saying AI is moving faster than we're able to govern it. We've been hearing for several months now ideas about how the federal government should be governing AI, but AI is developing faster than we're able to. We've been at this for months. Other Senate

Le sénateur Boudreau : J'ai une petite question pour Mme Dassa et une autre pour M. Menezes.

Madame Dassa, vous avez déclaré, dans votre déclaration liminaire, que la souveraineté des données est impérative — je paraphrase. Vous avez beaucoup insisté sur ce point. Toutefois, nous avons entendu dire que la CLOUD Act états-unienne rend cela totalement impossible, car le gouvernement américain — ma collègue vient d'en parler — peut déjà contraindre d'autres pays à lui remettre leurs données. Que répondez-vous à cela? La souveraineté des données est-elle possible avec la CLOUD Act?

Mme Dassa : En un mot, oui. L'important, ce n'est pas seulement l'endroit où se trouvent les données, mais aussi le système juridique qui régit le propriétaire qui gère ces données ou y accède.

Il arrive, si un prestataire de services a son siège social dans un pays étranger ou relève juridiquement de celui-ci, que ce pays ait des lois permettant aux autorités à demander les données détenues ou contrôlées par ce prestataire. Tout dépend de la manière dont le service est structuré.

Nous en revenons donc à la manière d'adopter l'intelligence artificielle appliquée de façon sûre et fiable, avec une gouvernance appropriée. Pour ce qui est de la souveraineté — dans la mesure où elle est possible —, on s'intéresse à ceux qui contrôlent l'infrastructure et aux lois qui encadrent l'exploitation de l'infrastructure. C'est pourquoi il est crucial que les données transitent par des réseaux situés sur le sol canadien, où le traitement informatique est réglementé, géré et contrôlé, et où les tribunaux canadiens ont compétence pour statuer sur les demandes d'accès.

Les trois éléments qui comptent ont donc plus à voir avec la gouvernance qu'avec l'engagement. Les réseaux doivent être souverains. C'est déjà notre cas, car nos données doivent être gérées de manière à ce que nous contrôlions leur circulation et le lieu où elles sont traitées. De plus, nos centres de données doivent être alimentés par de l'énergie canadienne afin que nous ayons pleins pouvoirs à chaque étape, ainsi que sur l'infrastructure informatique qui alimente les charges de travail d'intelligence artificielle. C'est à la fois possible et réalisable.

Nous disposons de ces ressources ici au Canada. Cependant, nous pouvons aussi nous conduire en bon citoyen du monde et collaborer avec d'autres fournisseurs de technologies mondiaux, pour peu que nous gardions le contrôle sur ces éléments et ces niveaux, ce qui est parfaitement faisable.

Le sénateur Boudreau : Monsieur Menezes, vous avez dit en partant que l'intelligence artificielle évolue au fond plus vite que nous ne sommes capables de la réguler. Depuis maintenant plusieurs mois, nous écoutons des suggestions sur la façon dont le gouvernement fédéral devrait réguler l'intelligence artificielle,

committees have been on this topic as well. It will take many more months for the government to even respond to our recommendations that will come out of this report.

How do you square that circle? How can you govern something that's moving faster than you are?

Mr. Menezes: Government needs to move away from trying to get a perfect framework for AI; that will be the case of death.

The committee needs to come up with two or three basic principles that you can start to adapt right away, implement baby steps and then evolve.

If you spend the next six months trying to build a perfect framework, by the time you build that framework, it will be obsolete. Then you will spend another six months doing it again. I know it is not the way government operates, but in the case of AI, that's the only way we are going to succeed. You have to come up with guidelines. It's the same way we're running our business.

We are figuring out that we need tools. These tools are pretty good; we are going to use them and implement them. Then, three months later, we find out that it's not doing what we want so we have to change. So you have to pivot. We have a pivoting strategy. I don't know how government and this committee can do it because it's not your way of doing things. It is going to be difficult.

Senator Arnold: Ms. Dassa, first of all, you were cut off at the very end. Is there anything you haven't covered that you wanted to express?

Ms. Dassa: Thank you for the offer. I've made all of my key points. I will reiterate that sovereignty is possible if we look at the multiple layers that are involved in the tech stacks that make a global AI. That's because there are multiple layers in a tech stack. What matters are networks, data centres, compute and governance, and that we have the ability to have all of that governed and controlled within Canada so that we are not subject to the jurisdiction of certain foreign actors, particularly to the south of our border.

But it is important to keep in mind, and to the previous comments around the speed that this is going, that countries that industrialize AI domestically will capture productivity gains, they will build globally competitive companies, and they will convert that digital capability into geopolitical strength.

mais celle-ci se développe à une vitesse que nous n'arrivons pas à suivre. Nous travaillons sur ce dossier depuis des mois. D'autres comités sénatoriaux se sont également penchés sur ce sujet. Il faudra encore de nombreux mois avant que le gouvernement parvienne à réagir aux recommandations qui découleront de ce rapport.

Comment concilier ces deux aspects? Comment peut-on réguler quelque chose qui évolue plus vite que nous?

M. Menezes : Le gouvernement doit abandonner l'idée de mettre en place un cadre parfait pour l'intelligence artificielle; il ne réussira pas de son vivant.

Le comité doit définir deux ou trois principes fondamentaux que vous pourrez commencer à adapter dès maintenant, mettre en œuvre petit à petit et ensuite continuer à développer.

Si vous passez les six prochains mois à essayer de mettre en place un cadre parfait, le temps que vous y parveniez, ce cadre sera déjà obsolète. Vous passerez alors six mois supplémentaires à tout refaire. Je sais que le gouvernement ne fonctionne pas ainsi, mais c'est la seule façon d'y parvenir dans le domaine de l'intelligence artificielle. Il faut établir des lignes directrices. C'est exactement comme ça que nous gérons notre entreprise.

Nous nous rendons compte que nous avons besoin d'outils. Ces outils sont plutôt efficaces; nous allons les utiliser et les mettre en œuvre. Puis, trois mois plus tard, nous constatons qu'ils ne produisent pas les résultats escomptés et nous devons donc faire des changements. Il faut donc s'adapter. Nous avons une stratégie d'adaptation. Je ne sais pas comment le gouvernement et le comité pourront y parvenir, car ce n'est pas votre façon de faire les choses. Ce sera difficile.

La sénatrice Arnold : Madame Dassa, pour commencer, vous avez été interrompue à la toute fin. Y a-t-il quelque chose que vous n'avez pas abordé, mais que vous teniez à ajouter?

Mme Dassa : Je vous remercie de votre offre. J'ai présenté tous mes arguments principaux. Je tiens à réaffirmer que la souveraineté est possible si l'on examine les multiples couches que comportent les piles technologiques utilisées pour créer une intelligence artificielle mondiale. C'est parce qu'une pile technologique comporte plusieurs couches. Ce qui est important, ce sont les réseaux, les centres de données, la puissance de calcul et la gouvernance, et le fait que nous ayons la capacité de régir et de contrôler tout cela au Canada afin de ne pas relever de la compétence de certains acteurs étrangers, en particulier au sud de notre frontière.

Toutefois, compte tenu des observations précédentes concernant la rapidité avec laquelle les choses évoluent, il est important de garder à l'esprit que les pays qui se dotent d'une industrie nationale de l'intelligence artificielle bénéficieront de gains de productivité, créeront des entreprises concurrentielles à

If we hesitate and we do not, we will depend on foreign infrastructure, and we will cede even more control and geopolitical strength to foreign actors. So we can't delay in taking action; we just need to do it intelligently, with governance, trust and safety at the forefront in the layers that do matter.

Senator Arnold: You didn't mention hardware at all. How important is that?

Ms. Dassa: By hardware, are you referring to the data centres themselves and the compute infrastructure?

Senator Arnold: The chips.

Ms. Dassa: That is very key.

Senator Arnold: Another question for you: In your day-to-day work, how do you balance safety versus innovation? That's something that comes up over and over again. How do we balance that? I'm wondering if you have a story.

Ms. Dassa: Yes, absolutely. I appreciate the question.

I operate in the applied AI world, which means that, where we operate, we ground all of our AI-powered experiences in trusted data sets. We are continuously advising the organizations and institutions that we work with on how to formulate that data strategy. So they make sure that governance and trust are rendered in every AI experience.

Yes, there is still hallucination that occurs, but within a controlled environment, and by leveraging models and architecture that allows for you to control that, it is kept at a minimum and within risk tolerance boundaries. So it is all around how you deploy the applied AI, and for which use cases you look to do that.

Speed is of the essence. We know there are use cases that allow us to leverage AI in a safe, trustworthy way. As long as we adopt those and learn as we go, as John mentioned, on the others, we will continue to progress. We do not need to start with the most risky or most unknown use cases.

l'échelle mondiale et transformeront ces capacités numériques en puissance géopolitique.

Si nous hésitons et ne faisons pas de même, nous dépendrons des infrastructures étrangères et céderons encore plus de contrôle et de puissance géopolitique à des acteurs étrangers. Nous ne pouvons donc pas tarder à agir; nous devons simplement le faire de manière intelligente en plaçant la gouvernance, la confiance et la sécurité au premier plan dans les domaines qui comptent vraiment.

La sénatrice Arnold : Vous n'avez pas du tout parlé du matériel. Quelle en est l'importance?

Mme Dassa : Par matériel, parlez-vous des centres de données eux-mêmes et des infrastructures informatiques?

La sénatrice Arnold : Les puces.

Mme Dassa : Elles sont vraiment essentielles.

La sénatrice Arnold : Voici une autre question pour vous : dans votre travail quotidien, comment conciliez-vous la sécurité et l'innovation? C'est un sujet qui revient sans cesse. Comment trouver le juste équilibre? Je me demande si vous avez une anecdote à ce sujet.

Mme Dassa : Oui, absolument. Je vous remercie de votre question.

Je travaille dans le secteur de l'intelligence artificielle appliquée, ce qui signifie que, dans notre secteur, toutes nos expériences fondées sur l'intelligence artificielle s'appuient sur des ensembles de données fiables. Nous conseillons sans cesse les organisations et les institutions avec lesquelles nous travaillons sur la manière d'élaborer cette stratégie en matière de données. Elles s'assurent ainsi que la gouvernance et la confiance font partie de chaque expérience en matière d'intelligence artificielle.

Oui, des fabulations d'intelligence artificielle se produisent encore, mais elles ont lieu dans un environnement contrôlé. En s'appuyant sur des modèles et une architecture qui permettent de les maîtriser, elles sont réduites au minimum et maintenues dans les limites de la tolérance au risque. Tout dépend donc de la manière dont vous déployez l'intelligence artificielle appliquée et des cas d'utilisation pour lesquels vous comptez l'utiliser.

La rapidité est essentielle. Nous savons qu'il existe des cas d'utilisation qui nous permettent de tirer parti de l'intelligence artificielle de manière sûre et fiable. Tant que nous adoptons ces cas d'utilisation et que nous tirons des leçons des autres au fur et à mesure, comme l'a mentionné M. Menezes, nous continuerons à progresser. Nous n'avons pas besoin de commencer par les cas d'utilisation les plus risqués ou les moins connus.

There is so much that AI can do in a controlled environment that still leads to transformative productivity gains that enhance competitive advantage. I see that every day with the institutions and organizations I advise and work with; too little of which are Canadian, unfortunately.

Senator Arnold: Thank you.

Senator Cuzner: Technology has been frightening for a long time now. I recall that, back at the turn of the century, with all the talk around the Y2K bug, my eight-year-old son at the time was convinced that when the clock struck 12, a giant eight-legged creature was going to march down Commercial Street in Glace Bay. It didn't work out that way, but we have received some serious and challenging information to date in this study.

Let's talk about the fears relating to workforce changes and workforce development. You said you are in the midst of it now; it is not something in the future. Obviously, your marketing team is nervous, anticipating layoff notices.

How is the workforce adapting? Have you seen losses or departments that have become redundant? Are you retraining? Are you doing in-house training? Are there organizations or institutions that you're relying on to help you with retooling your workforce?

The Chair: Senator Cuzner, would you like to hear from Mr. Richer on this as well?

Senator Cuzner: Yes.

Mr. Menezes: At Bell Cyber, we are cybersecurity experts. We have asked how we can use AI to make cybersecurity better because our attacking hackers are using AI. So we have to use AI. We've tried to change the mindset of our people.

You will find that 20% of the workforce adapt to AI very quickly, and 80% of the workforce is not moving. Will there be job losses? Probably there will be job losses in one sector and job gains in another sector.

When you talk about data governance, at Bell AI, we are working with Cohere, which is a Canadian-based LLM company, and we're putting cybersecurity on the Cohere LLMs, running on the Bell AI Fabric, which is running on the Bell network. So we

L'intelligence artificielle est capable d'accomplir une multitude de tâches dans un environnement contrôlé, ce qui se traduit par des gains de productivité transformateurs qui renforcent l'avantage concurrentiel. J'en suis témoin tous les jours dans les institutions et les organisations que je conseille et avec lesquelles je travaille; malheureusement, trop peu d'entre elles sont canadiennes.

La sénatrice Arnold : Merci.

Le sénateur Cuzner : La technologie fait peur depuis bien longtemps déjà. Je me souviens qu'au tournant du siècle, alors que tout le monde parlait du bogue de l'an 2000, mon fils, qui avait alors 8 ans, était persuadé qu'à minuit, une créature géante à huit pattes allait défiler dans la rue Commercial, à Glace Bay. Les choses ne se sont pas passées ainsi, mais cette étude nous a livré jusqu'à présent des informations sérieuses et problématiques.

Parlons des craintes liées aux changements d'effectif et au perfectionnement de la main-d'œuvre. Vous avez dit que vous étiez en train de mettre cela en œuvre en ce moment; ce n'est pas quelque chose qui se produira à l'avenir. De toute évidence, votre équipe de marketing est inquiète et s'attend à des licenciements.

Comment la main-d'œuvre s'adapte-t-elle? Avez-vous constaté des pertes ou identifié des services qui sont devenus superflus? Procédez-vous au recyclage professionnel? Organisez-vous des formations internes? Y a-t-il des organisations ou des institutions sur lesquelles vous comptez pour vous aider à réorganiser votre main-d'œuvre?

La présidente : Sénateur Cuzner, souhaitez-vous également entendre l'avis de M. Richer à ce sujet?

Le sénateur Cuzner : Oui.

M. Menezes : À Bell Cyber, nous sommes des experts en cybersécurité. Nous nous sommes demandé comment utiliser l'intelligence artificielle pour améliorer la cybersécurité, car les pirates informatiques qui nous attaquent ont recours à l'intelligence artificielle. Nous devons donc nous aussi l'utiliser. Nous avons essayé de changer la mentalité de nos employés.

Vous constaterez que 20 % de la main-d'œuvre s'adapte très rapidement à l'intelligence artificielle, tandis que 80 % de cette main-d'œuvre demeure inchangée. Y aura-t-il des pertes d'emplois? Il y aura probablement des pertes d'emplois dans un secteur et des gains d'emplois dans un autre.

En ce qui concerne la gouvernance des données, IA Bell collabore avec Cohere, une entreprise canadienne de grands modèles de langage, et intègre la cybersécurité dans les grands modèles de langage de Cohere, qui fonctionnent sur le Réseau

have the infrastructure in place for sovereign AI capability. Mr. Richer, if you can add to what we're doing with Bell AI Fabric, that would be great.

Michel Richer, President, Bell AI, Bell Canada: There are two aspects to answering your question. The first thing is that we have discussed a lot so far today about the concerns. The reason AI is moving so fast is because a very broad group of business leaders, including ourselves, sees incredible potential in the benefits of adopting AI. It is this balance of both where there are risks in the adoption of AI, but there is an even greater risk in not adopting it because then we can't move at pace with the speed at which the entire world is evolving right now.

At Bell, we are enabling our entire workforce to work with AI by providing them with the right tools and providing very clear policy around the responsible use of AI that we deployed three years ago, and we are constantly evolving it as we understand better how we're going to use AI.

From an enablement perspective, we are doing it in two ways. There is a general enablement, where we believe every employee needs to start using AI in some aspect of their work. This is the general use of AI that you see with large language models and basic agents. We are also seeing specific functions in some departments where the use cases are already transformational, where we are doubling down on enabling those employees faster by transforming the workflow and processes by which we deliver services to our customers or manage our infrastructure.

Senator Cuzner: Has there been a loss of jobs in those sectors?

Mr. Richer: There is constant evolution of the fabric of our workforce. There are many cases where we are enabling people to do their job in ways they couldn't before. For example, in our customer operations in our call centres, we want to coach our agents to follow our processes and give good service to our customers. If you go back only a few years, we used to have people listen to calls in order to be able to give feedback to the agents.

We listened to a fraction of 1% of calls. As of today, we are able to use AI and listen to about 95% of the calls in a very effective way and understand if the agents are following the process and giving the right service. Then we are able to give coaching to all of our agents so they improve. We are still doing

d'IA tissé, qui fonctionne lui-même sur le réseau de Bell. Nous disposons donc des infrastructures nécessaires pour une capacité d'intelligence artificielle souveraine. Monsieur Richer, ce serait formidable si vous pouviez nous en dire plus sur ce que nous faisons avec le Réseau d'IA tissé.

Michel Richer, président, IA Bell, Bell Canada : Il y a deux aspects à prendre en compte pour répondre à votre question. Tout d'abord, nous avons beaucoup discuté aujourd'hui des préoccupations. Si l'intelligence artificielle évolue si rapidement, c'est parce qu'un très grand nombre de chefs d'entreprise, y compris nous, reconnaissent l'incroyable potentiel des avantages liés à son adoption. Il s'agit de trouver un équilibre entre les risques liés à l'adoption de l'intelligence artificielle et le risque encore plus grand de ne pas l'adopter, car cela nous empêcherait de suivre le rythme auquel le monde entier évolue actuellement.

Chez Bell, nous permettons à tous nos employés de travailler avec l'intelligence artificielle en leur fournissant les bons outils et en mettant en place il y a trois ans une politique très claire concernant l'utilisation responsable de l'intelligence artificielle que nous adaptons constamment à mesure que nous comprenons mieux comment nous allons utiliser cette technologie.

Pour ce qui est d'encourager l'adoption de l'intelligence artificielle, nous procédons de deux manières. Il y a une approche générale, selon laquelle nous estimons que chaque employé doit commencer à utiliser l'intelligence artificielle dans certains aspects de son travail. Il s'agit là de l'utilisation générale de l'intelligence artificielle que l'on observe avec les grands modèles de langage et les agents de base. Nous observons également des fonctions précises dans certains services où les cas d'utilisation sont déjà source de transformation et où nous redoublons d'efforts pour permettre à ces employés de se familiariser plus rapidement avec l'intelligence artificielle en transformant les flux de travail et les processus par lesquels nous fournissons des services à nos clients ou gérons notre infrastructure.

Le sénateur Cuzner : Y a-t-il eu des pertes d'emplois dans ces secteurs?

M. Richer : Notre main-d'œuvre est en constante évolution. Dans de nombreux cas, nous permettons à nos employés de faire leur travail d'une manière qui leur était auparavant impossible. Par exemple, dans nos services à la clientèle au sein de nos centres d'appels, nous souhaitons apprendre à nos agents à respecter nos procédures et à offrir un service de qualité à nos clients. Il y a encore quelques années, des personnes étaient chargées d'écouter des appels afin de pouvoir donner de la rétroaction aux agents.

Nous n'écoutions qu'une fraction de 1 % des appels. Aujourd'hui, grâce à l'intelligence artificielle, nous sommes en mesure d'écouter environ 95 % des appels de manière très efficace et de vérifier si les agents respectent le processus et fournissent un service de qualité. Nous pouvons ensuite encadrer

the same thing, but now we are doing it exponentially better than we used to do it.

The Chair: Thank you.

Senator Petitclerc: I have one question. I'm not sure who will jump in, but I'm wondering about accountability. I was listening to you, Mr. Menezes, and it is a little scary. When AI systems go into public service or private industry, we have the government that has a role and the guardrails. If something fails — because we were talking about agents gaining autonomy or initiative — who then is held accountable? Is it the government with the guardrails? Is it the developers? Is it the operators? I'm not sure who wants to jump in on how they see that?

Ms. Dassa: It depends on who is deploying the language models. If we are deploying an agent within the Bell Cyber environment, and one of our agents goes rogue, then it is my responsibility. That's because the agent is almost like my employee. What do you do when you have an employee go rogue or commit fraud? It is the same thing. As a matter of fact, there is a school of thought that says the agent should be treated like humans, and you should have HR policies for agents. That is where we're going with that.

Senator Petitclerc: So it is not the guardrails.

Mr. Menezes: The guardrails are tools. You hire somebody, and say, you can do this within your job. You can do this, and you have HR policies. You have other health and safety policies. When the employee doesn't do what you tell them to do or doesn't follow policy, what do you do?

Senator Petitclerc: I don't know if the other witnesses would have anything to say about this. I know it is not specifically what you talked about, but I'm looking for input on accountability.

Mr. Richer: One element I would add very quickly is that, as part of each of the responsibility AI policies you will see deployed across organizations, there is always a pillar in transparency. As we think of agents, models and data systems, in some cases, because of the speed of evolution, it's difficult to understand exactly why they behave in a certain way. But the importance of all of the actors being committed to understanding how they behave and being able to adapt as a function of that is one of the key guardrails that we all have.

tous nos agents afin qu'ils s'améliorent. Nous faisons toujours la même chose, mais nous la faisons désormais bien mieux qu'auparavant.

La présidente : Merci.

La sénatrice Petitclerc : J'ai une question. Je ne sais pas qui va y répondre, mais je m'interroge sur la question de la reddition de comptes. Je vous écoutais, monsieur Menezes, et cela fait un peu peur. Lorsque les systèmes d'intelligence artificielle sont déployés dans le secteur public ou privé, le gouvernement a un rôle à jouer et met en place des garde-fous. Si quelque chose tourne mal — puisque nous parlions d'agents qui acquièrent de l'autonomie ou de l'initiative —, qui est alors tenu responsable? Est-ce le gouvernement avec ses garde-fous? Est-ce les développeurs? Est-ce les exploitants? Je ne sais pas qui souhaite prendre la parole pour donner son point de vue à ce sujet.

Mme Dassa : Tout dépend de qui déploie les modèles de langage. Si nous déployons un agent au sein de l'environnement Bell Cyber et que l'un de nos agents décide de se rebeller, c'est alors ma responsabilité. En effet, cet agent est presque comme un de mes employés. Que faites-vous lorsqu'un de vos employés se rebelle ou fait de la fraude? C'est exactement la même chose. En fait, certains pensent que les agents devraient être traités comme des êtres humains et qu'il faudrait mettre en place des politiques en matière de ressources humaines pour eux. C'est la direction que nous prenons.

La sénatrice Petitclerc : Ce ne sont donc pas les garde-fous.

M. Menezes : Les garde-fous sont des outils. Vous embauchez quelqu'un et vous lui dites ce qu'il peut faire dans le cadre de son travail. Il peut faire telle ou telle chose et il y a des politiques en matière de ressources humaines. Il y a d'autres politiques en matière de santé et de sécurité. Que faites-vous lorsque l'employé ne fait pas ce que vous lui demandez ou ne respecte pas les politiques?

La sénatrice Petitclerc : Je ne sais pas si les autres témoins ont quelque chose à dire à ce sujet. Je sais que ce n'est pas exactement ce dont vous avez parlé, mais j'aimerais avoir votre avis sur la question de la responsabilité.

M. Richer : J'ajouterais une chose, très rapidement : dans chacune des politiques de responsabilité en matière d'intelligence artificielle mises en œuvre au sein des organisations, la transparence constitue toujours un pilier essentiel. En ce qui concerne les agents, les modèles et les systèmes de données, il est parfois difficile, en raison de la rapidité de leur évolution, de comprendre exactement pourquoi ils se comportent d'une certaine manière. Cela dit, l'importance pour tous les acteurs de s'engager à comprendre leur comportement et d'être capables de s'adapter en fonction de celui-ci constitue l'une des principales mesures de sauvegarde pour nous tous.

Ms. Dassa: As part of governance, there is a strong emphasis on the ability to have observability throughout how the AI acts.

Going back to your earlier question, accountability is shared in layers. The organization deploying the AI system has a responsibility for how that system is used, the decisions that they allow it to support and the outcomes they allow it to produce. This is similar to any other operational tool. If the bank uses AI in lending decisions, they are accountable for that. But that is where shaping guardrails have been thoroughly tested and are controllable. The technology providers and developers you alluded to are responsible for the design and reliability of the system: those safety mechanisms and guardrails, that observability, capability and transparency about the capability and the limitations. If there is a failure due to a defect or misrepresentation, accountability can extend to the provider.

Finally, the regulatory framework by the government: Government's role is to define clear rules and standards, establish liability frameworks and ensure oversight and enforcement. So government is not accountable for individual system failures, of course, but for ensuring that the rules of the system are clear and are enforced.

This is why human oversight, controlled deployment environments and clear accountability frameworks are critical because autonomy does not remove accountability by any means.

Senator Petitclerc: Thank you for this.

The Chair: I want to insert a question. Earlier, you spoke about risk tolerance boundaries. I'm wondering if you can help us understand what you mean by that or what the role is, and how you see them becoming — you spoke as if they were important — our approach to accepting that there will be some risk in what we do with AI.

Ms. Dassa: Yes, indeed. When we test or pilot use cases with organizations, we have to establish risk tolerances. By that, I mean looking at understanding the accuracy and completeness of a question versus the answer rate. Organizations decide to what degree they make a trade-off in either having the answer rate be lower and accuracy be at the highest standards.

Mme Dassa : Dans le cadre de la gouvernance, on met particulièrement l'accent sur la capacité d'observer le comportement de l'intelligence artificielle dans son ensemble.

Pour revenir à votre question précédente, la responsabilité est répartie à plusieurs niveaux. L'organisation qui déploie le système d'intelligence artificielle est responsable de la manière dont ce système sera utilisé, des décisions qu'elle l'autorise à prendre et des résultats qu'elle l'autorise à produire. Cela vaut pour tout autre outil d'exploitation. Si la banque utilise l'intelligence artificielle pour ses décisions de crédit, elle en est responsable. C'est là que les mesures de sauvegarde ont été minutieusement testées et sont contrôlables. Les fournisseurs de technologie et les développeurs auxquels vous faites référence sont responsables de la conception et de la fiabilité du système : les mécanismes de sécurité, les mesures de sauvegarde, l'observabilité, les capacités et la transparence concernant les capacités et les limites. En cas de défaillance due à un défaut ou à des informations erronées, la responsabilité peut être étendue au fournisseur.

Enfin, le cadre réglementaire mis en place par le gouvernement : le rôle du gouvernement consiste à définir des règles et des normes claires, à établir des cadres de responsabilité et à superviser et faire respecter ces dispositions. Ainsi, le gouvernement n'est bien sûr pas responsable des défaillances individuelles du système, mais il doit veiller à ce que les règles du système soient claires et respectées.

Voilà pourquoi il est essentiel de maintenir une surveillance humaine, de disposer d'environnements de déploiement contrôlés et de mettre en place des cadres de responsabilité clairs, car l'autonomie ne nous libère pas de nos responsabilités, loin de là.

La sénatrice Petitclerc : Je vous remercie de votre réponse.

La présidente : J'aimerais poser une question. Tout à l'heure, vous avez évoqué les limites de la tolérance au risque. Je me demande si vous pourriez nous aider à comprendre ce que vous entendez par là, quel est leur rôle, et comment vous envisagez leur évolution — vous en avez parlé comme si elles étaient importantes — dans notre approche visant à accepter qu'il y aura une part de risque dans ce que nous faisons avec l'intelligence artificielle.

Mme Dassa : Oui, tout à fait. Lorsque nous effectuons des tests ou des projets pilotes avec des organisations, nous devons définir des seuils de tolérance au risque. J'entends par là qu'il s'agit d'évaluer la précision et l'exhaustivité d'une question par rapport au taux de réponse. Les organisations décident dans quelle mesure elles sont prêtes à faire un compromis entre un taux de réponse plus faible et une précision qui répond aux normes les plus élevées.

But one thing is certain: There are certain types of experiences or answers where there is a zero per cent tolerance on inaccuracy or incompleteness, and those hail back to what Mr. Menezes was referring to earlier, around anything that could be potentially dangerous or cause a breach of the safety of any individuals. There, there is no tolerance.

What I'm referring to is more about the ability of — for instance, from a customer service or support perspective — an agent to answer a customer's inquiry of a Canadian organization, fully grounded in policy or with some additional contextual interpretation. There are minimum thresholds beyond which we will not allow it to go, but organizations can play within a certain level of accuracy.

The Chair: Thank you very much.

Senator Hay: Ms. Dassa, I'm going to ask you about sovereignty and data risk. Again, getting back to the statement that Professor Stein made earlier in the week that sovereignty around data is not so much about control, but, rather, free from coercion. She was speaking about the U.S. CLOUD Act and trade-offs and choices one should make.

For example, a likely trade-off is that we will, in our AI stack, have to be working with the hyperscalers. It is just that we can't afford to have our own hyperscalers. Can you comment on that or respond to that?

Ms. Dassa: Certainly. Our data needs to be governed here. That is about ensuring that Canadian data is subject to Canadian laws only so that we decide how it is stored, how it moves within borders and, most importantly, across borders and who can access it. It is about that legal and regulatory control, not just physical location.

Senator Hay: If I could interject, because I'm not clear on it. If it is also a U.S. company, like, for example, AWS, which is a hyperscaler. AWS is in Montreal. Our Canadian data is in that data centre, and if the U.S. government declares an emergency, they can demand AWS data. Whatever data is in those pipes and in that data centre, regardless of whether it's on our soil, has to go to the U.S.

Toutefois, une chose est sûre : il y a certains genres d'expériences ou de réponses pour lesquelles la tolérance à l'inexactitude ou au manque de précision est nulle, et celles-ci renvoient à ce dont M. Menezes parlait tout à l'heure, à savoir tout ce qui pourrait être potentiellement dangereux ou compromettre la sécurité de quiconque. Là, il n'y a aucune tolérance.

Ce dont je parle concerne davantage la capacité d'un agent — par exemple, dans le cadre du service à la clientèle ou du soutien technique — à répondre à la demande d'un client d'une organisation canadienne, en s'appuyant pleinement sur les directives ou en y ajoutant une interprétation contextuelle. Il y a certains seuils au-delà desquels nous n'autoriserons pas le système à aller, mais les organisations peuvent avoir du jeu quant à la précision.

La présidente : Merci beaucoup.

La sénatrice Hay : Madame Dassa, j'aimerais vous interroger sur la souveraineté et les risques liés aux données. Pour revenir à la déclaration faite par Janice Stein en début de semaine, la question de la souveraineté des données ne porte pas tant sur le contrôle que sur l'absence de coercition. Elle parlait de la CLOUD Act des États-Unis, et des compromis et des choix que chacun doit faire.

Par exemple, il est probable que nous devions faire le compromis de travailler avec les fournisseurs de services infonuagiques à très grande échelle pour notre infrastructure d'intelligence artificielle. C'est simplement que nous ne pouvons pas nous permettre d'avoir nos propres fournisseurs de tels services. Pourriez-vous nous donner votre avis ou une réponse à ce sujet?

Mme Dassa : Tout à fait. Nos données doivent être gouvernées ici. Il s'agit de garantir que les données canadiennes soient régies exclusivement par la législation canadienne, afin que ce soit nous qui décidions comment elles sont stockées, comment elles circulent à l'intérieur du pays et, surtout, au-delà de nos frontières, ainsi que qui peut y avoir accès. C'est une question de contrôle juridique et réglementaire, et pas seulement d'emplacement physique.

La sénatrice Hay : Si je peux vous interrompre, je ne comprends pas bien. Prenons une entreprise américaine, comme AWS, qui est un fournisseur de services infonuagiques à très grande échelle. AWS est implantée à Montréal et nos données canadiennes se trouvent dans son centre de données. Si le gouvernement américain déclare une situation d'urgence, il peut exiger qu'AWS lui livre ses données. Toutes les données qui transitent par les réseaux et qui se trouvent dans ce centre de données, qu'elles soient ou non sur notre territoire, devraient être transmises aux États-Unis.

Ms. Dassa: There are specificities that allow for an international company, like AWS, to provide a shadow instance that is entirely governed in Canada. So whether it has AWS capabilities or not, what matters is that the data is governed within the scope and framework of that instance, and that the data doesn't cross over into jurisdictions. So it's all around how the data flows through and the instance itself of that engagement layer that they would create.

It doesn't need to be owned entirely when it comes outside of the compute or governance layer. There is the ability to have collaboration —

Senator Hay: But AWS would be required, through the U.S. CLOUD Act, to release the data, I believe.

Perhaps the Tier I defence data, for example, needs to be within a full Canadian, end-to-end tech stack or data environment. Would you agree?

Ms. Dassa: Again, where the data flows through and where it maintains, even if there is a Google or an AWS involved that is headquartered and LLC'd in the U.S., that doesn't change that if we had the right governance and legal entities established with them, then the U.S. data control act would not be applicable. There are ways of establishing that. I will admit I am not a legal expert.

The Chair: Thank you, Ms. Dassa.

Senator Senior: I will be very quick, and it's to Ms. Dassa again. You said something that triggered this question for me, which is that we need to have the ability to observe, and that is a human function you are speaking of, correct? Based on the speed of development in AI, do you imagine where observability could be AI observing AI?

Ms. Dassa: You can have that type of "mirror in front of the mirror" type of situation where AI can observe its own operations, but you always need a human-monitoring element to supersede. Again, it comes back to what use cases you are leveraging AI for.

Obviously, anything to do with defence is outside of what I'm discussing here. I'm really talking about applied AI use cases defined within operational questions, where there would be human monitoring involved always to ensure that the AI remains properly constrained, and, when deployed in the right way, there is no risk for it to go rogue with the right set of security constraints.

Mme Dassa : Certaines particularités permettent à une entreprise internationale comme AWS de fournir une instance « miroir » entièrement régie au Canada. Ainsi, qu'elle intègre ou non les fonctionnalités d'AWS, ce qui importe, c'est que les données soient gérées dans le cadre et selon les règles de cette instance, et qu'elles ne franchissent pas les frontières nationales. En définitive, tout repose sur la manière dont les données circulent et sur l'interface qui serait mise en place elle-même.

Il n'est pas nécessaire d'être propriétaire à part entière des couches autres que celles du calcul ou de la gouvernance. Il est possible de collaborer...

La sénatrice Hay : Néanmoins, je pense qu'AWS serait tenue, en vertu de la CLOUD Act des États-Unis, de communiquer les données.

Peut-être que les données relatives à la défense de niveau I, par exemple, devraient se trouver dans un environnement technologique ou de données entièrement canadien, de bout en bout. Êtes-vous d'accord?

Mme Dassa : Encore une fois, quel que soit le lieu de transit ou de stockage des données, même si une entreprise comme Google ou AWS, dont le siège social est situé aux États-Unis et qui y est enregistrée en tant que société à responsabilité limitée, est impliquée, cela ne change rien au fait que, si nous travaillons avec elle pour mettre en place une gouvernance adéquate et si nous créons les entités juridiques appropriées, la loi américaine sur le contrôle des données ne sera pas applicable. Il y a des moyens d'y parvenir. Je reconnais que je ne suis pas juriste.

La présidente : Merci, madame Dassa.

La sénatrice Senior : Je serai très brève, et je m'adresse à nouveau à Mme Dassa. Vous avez dit quelque chose qui m'a amenée à poser la question suivante. Vous avez dit que nous devons être capables d'observer, et vous parlez là d'une fonction humaine, n'est-ce pas? Compte tenu de la rapidité des progrès en matière d'intelligence artificielle, imaginez-vous que la capacité d'observation pourrait un jour consister en une intelligence artificielle qui observe une autre intelligence artificielle?

Mme Dassa : On peut se retrouver dans une situation de type miroir, où l'intelligence artificielle est capable d'observer son propre fonctionnement, mais il faut toujours qu'un élément de surveillance humaine puisse s'imposer. Encore une fois, tout dépend de l'usage que vous faites de l'intelligence artificielle.

Évidemment, ce dont je parle exclut tout ce qui touche à la défense. En fait, je parle de cas où l'intelligence artificielle est utilisée dans le cadre de questions opérationnelles, où il y aurait toujours une supervision humaine pour veiller à ce qu'elle reste correctement encadrée et où, lorsqu'elle est déployée de manière adéquate, il n'y a aucun risque qu'elle devienne incontrôlable, sous réserve des contraintes de sécurité appropriées.

For any other more fantastical potential use cases, I'll defer to those experts. But when it comes to the use cases in applied AI that are generating productivity gains and allowing organizations to have their people focus on more strategic work, observability is in-built into those solutions.

Senator Senior: Thank you. Is there any comment on that from Mr. Menezes or Mr. Richer?

Mr. Menezes: What we are doing in Cyber is looking for anomalies in how the AI is operating. So, yes, you can have an AI looking at the AI, but you look at the anomalies, and then humans look at the anomalies and can do a more in-depth investigation.

Even in our own system, we run an autonomous SOC, and we have all these agents working, but we have guardrails in place and systems in place so that if there is confusion or disagreement among the agents, after a certain number of tries, it will flip out an incident and allow a human to intervene and make a decision.

But we're still learning. I keep repeating that. We're still learning because we don't know yet.

Senator Senior: Thank you very much.

The Chair: Thank you very much.

This brings us to the end of today's panel. I would like to thank all the witnesses who brought your testimony to us today and shared your wisdom.

During yesterday's meeting at committee, the committee adopted all 11 clauses of the bill. When the committee arrived at the adoption of the preamble, an amendment was moved, and subsequently, that amendment was withdrawn. Today, we will continue from that point.

Senators, is it agreed that the committee continue with the clause-by-clause consideration of Bill S-5, An Act respecting the interoperability of health information technology and to prohibit data blocking by health information technology vendors?

Hon. Senators: Agreed.

The Chair: Senators, shall the preamble carry?

[*Translation*]

Senator Petitclerc: Colleagues, I would like to propose an amendment.

Pour tout autre scénario d'utilisation plus fantaisiste, je m'en remettrai aux experts. Toutefois, en ce qui concerne les produits d'intelligence artificielle appliquée qui génèrent des gains de productivité et qui permettent aux organisations d'utiliser leurs employés pour des tâches plus stratégiques, ceux-ci comprennent une fonction d'observabilité par défaut.

La sénatrice Senior : Merci. MM. Menezes et Richer ont-ils quelque chose à ajouter?

M. Menezes : Au sein de Bell Cyber, nous cherchons à détecter les anomalies dans le fonctionnement de l'intelligence artificielle. Oui, il est possible de faire en sorte qu'une intelligence artificielle surveille une autre intelligence artificielle, mais l'objectif est de repérer les anomalies, qui sont ensuite examinées par des humains afin qu'on puisse mener une enquête plus approfondie.

Même dans notre propre système, nous gérons un centre d'opérations de sécurité autonome où travaillent de nombreux agents, mais nous avons mis en place des mesures de protection et des systèmes qui font que, s'il y a une confusion ou un désaccord entre les agents, après un certain nombre de tentatives, le système signalera un incident et permettra à un humain d'intervenir pour prendre une décision.

Toutefois, nous sommes toujours en phase d'apprentissage. Je ne cesse de le répéter. Nous continuons d'apprendre parce que nous ne savons pas encore.

La sénatrice Senior : Merci beaucoup.

La présidente : Merci beaucoup.

Ceci conclut les témoignages pour aujourd'hui. Je remercie les témoins qui nous ont fait profiter de leur sagesse aujourd'hui.

Pendant la réunion d'hier, le comité a adopté l'ensemble des 11 articles du projet de loi. Lorsque le temps est venu d'adopter le préambule, un amendement a été proposé, puis retiré par la suite. Aujourd'hui, nous reprendrons à ce stade.

Plaît-il aux sénateurs que le comité poursuive l'examen article par article du projet de loi S-5, Loi concernant l'interopérabilité des technologies de l'information sur la santé et visant à interdire le blocage de données par les fournisseurs de technologies de l'information sur la santé?

Des voix : D'accord.

La présidente : Sénateurs, le préambule est-il adopté?

[*Français*]

La sénatrice Petitclerc : Chers collègues, j'aimerais proposer un amendement.

I move:

That Bill S-5 be amended in the preamble,

(a) on page 1,

(i) by replacing line 29 with the following:

"Whereas Parliament wishes to promote coopera-",

(ii) by replacing line 31 with the following:

"territorial governments, First Nations, Inuit and Métis Peoples and key";

(b) on page 2, by adding the following before line 1:

"And whereas Parliament affirms that the enabling of easy, complete and secure access to and use and exchange of electronic health information and the governance of data under this Act as that data relates to First Nations, Inuit and Métis Peoples must occur in a manner that respects Indigenous data sovereignty;".

Je propose :

Que le projet de loi S-5 soit modifié, au préambule, à la page 2 :

a) par substitution, à la ligne 5, de ce qui suit :

« et territoriaux, les peuples des Premières Nations, des Inuits et des Métis et les princi- »;

par substitution, à la ligne 8, de ce qui suit :

« de santé connecté;

qu'il déclare que les mesures autorisées par la présente loi visant l'utilisation et l'échange de renseignements électroniques sur la santé, l'accès facile, complet et sécuritaire à ces renseignements et la gouvernance des données en ce qui a trait aux peuples des Premières Nations, des Inuits et des Métis doivent respecter la souveraineté des données autochtones, ».

Sénateurs, cet amendement est présenté aujourd'hui au nom de la sénatrice Greenwood. La sénatrice Greenwood a dit hier que la partie a)(i) de l'amendement, dans la version anglaise, correspondait à une modification de mise en forme visant à déplacer le mot « and » sur une autre ligne dans le préambule. La partie a)(ii) de l'amendement fait suite à l'intervention d'une témoin qui a demandé au comité de reconnaître la distinction faite dans la collecte des données et de remplacer l'expression « peuples autochtones » par « peuples des Premières Nations, des Inuits et des Métis ».

Comme l'a indiqué hier la sénatrice Greenwood, l'amendement utilise également, en anglais, un P majuscule dans le mot « Peoples » afin de refléter les changements linguistiques qui reconnaissent l'existence de sociétés multiples et distinctes au Canada. Ce libellé est également conforme au guide de rédaction en anglais disponible sur le portail de la rédaction du gouvernement du Canada.

[*English*]

Senators, this amendment is introduced today on behalf of Senator Greenwood. Senator Greenwood said yesterday that part (a)(i) of the amendment in the English component is a formatting requirement that moves the word “and” to a different line in the preamble. Part (a)(ii) of the amendment is in response to a witness who called upon the committee to recognize the distinctions-based nature of data collection and amend the term “Indigenous Peoples” to “First Nation, Inuit and Métis Peoples.”

As Senator Greenwood said yesterday, the amendment also uses a capital P in the word “Peoples” to reflect the evolving language recognizing the multiple, distinct societies within Canada. This language is also consistent with the language guide found on the Government of Canada’s writing portal.

Part (b) of the amendment was informed by the testimony of multiple witnesses. Yesterday, Senator Greenwood quoted many of those witnesses, discussing their testimony at length in our committee meeting. Based on the discussion yesterday with officials on the language of this section, it has been revised to use language that is more consistent with the text describing the purpose of the bill found in clause 3.

I would also like to mention that Senator Greenwood supports the wording of this new amendment. She is satisfied that it advances the concept of Indigenous data sovereignty and is content with the knowledge that this will be the first time the concept will be used in Canadian law.

The Chair: I open the floor for discussion. Are there any comments?

Seeing no comments, senators, shall the amendment carry?

Hon. Senators: Agreed.

The Chair: Senators, shall the preamble, as amended, carry?

Hon. Senators: Agreed.

The Chair: Senators, shall the title carry?

Hon. Senators: Agreed.

The Chair: Shall the bill, as amended, carry?

Hon. Senators: Agreed.

The Chair: Is it agreed that the law clerk and parliamentary counsel be authorized to make necessary technical, grammatical and other required non-substantive changes resulting from the amendments adopted by the committee today in both official languages, including the updating, cross-referencing and renumbering of provisions?

[*Traduction*]

La partie b) de l’amendement s’appuie sur les témoignages de plusieurs témoins. Hier, la sénatrice Greenwood a cité bon nombre de ces témoins et a longuement commenté leurs témoignages pendant les audiences de ce comité. À la suite de la discussion d’hier avec le personnel au sujet du libellé de cette partie, elle a été modifiée afin d’adopter une formulation plus conforme au libellé de l’article 3, qui décrit l’objet du projet de loi.

Je précise également que la sénatrice Greenwood approuve le libellé de ce nouvel amendement. Elle estime qu’il fait progresser le concept de souveraineté des données autochtones et elle se réjouit que ce concept soit pour la première fois intégré dans la législation canadienne.

La présidente : Quelqu’un veut-il intervenir?

Je n’entends aucune voix s’élever. Sénateurs, l’amendement est-il adopté?

Des voix : D’accord.

La présidente : Sénateurs, le préambule modifié est-il adopté?

Des voix : D’accord.

La présidente : Sénateurs, le titre est-il adopté?

Des voix : D’accord.

La présidente : Le projet de loi modifié est-il adopté?

Des voix : D’accord.

La présidente : Est-il convenu que le légiste et conseiller parlementaire soit autorisé à apporter toute modification mineure, notamment technique ou grammaticale, rendue nécessaire par suite de l’adoption des amendements par le comité, dans les deux langues officielles, y compris la mise à jour des renvois et la renumérotation des dispositions?

Hon. Senators: Agreed.

The Chair: Senators, does the committee wish to consider appending observations to the report?

Hon. Senators: Agreed.

The Chair: The rules allow us to go in camera to discuss these observations and subsequently consider a draft report. Is it agreed that the committee proceed in camera?

Hon. Senators: Agreed.

(The committee continued in camera.)

Des voix : D'accord.

La présidente : Sénateurs, le comité souhaite-t-il examiner la possibilité d'ajouter des observations au rapport?

Des voix : D'accord.

La présidente : Le Règlement nous autorise à nous retirer à huis clos pour examiner ces observations, puis examiner un projet de rapport. Le comité souhaite-t-il examiner ces observations à huis clos?

Des voix : D'accord.

(La séance se poursuit à huis clos.)