Clé de correction

Test provincial

Français arts langagiers – immersion
12e année (40S)

Compréhension

L’empreinte numérique : rêve ou cauchemar?

Janvier 2025

Manitoba

Données de catalogage avant publication – Éducation et Apprentissage de la petite enfance Manitoba

Test provincial, Français arts langagiers – immersion, 12e année (40S).
[ressource électronique]. Clé de correction : Compréhension – Janvier 2025.

1. Français (Langue) – Examens.
2. Tests et mesures en éducation – Manitoba.
3. Français (Langue) – Français écrit – Test d'aptitude – Manitoba.
I. Manitoba. Éducation et Apprentissage de la petite enfance Manitoba.
448.0076

Éducation et Apprentissage de la petite enfance Manitoba
Bureau de l'éducation française
Winnipeg (Manitoba) Canada

Les sites Web mentionnés dans le présent document pourraient faire l'objet de changement sans préavis.

Les opinions et les idées exprimées dans les ouvrages reproduits dans le présent cahier peuvent représenter le point de vue des auteurs et ne reflètent pas nécessairement la position du gouvernement du Manitoba. Les ouvrages ont été choisis dans le but d'exposer les élèves à une variété de perspectives relatives au thème du test.

Dans le présent document, le genre masculin appliqué aux personnes est employé sans aucune discrimination et uniquement dans le but d'alléger le texte.

Table des matières

Introduction

Le *Test provincial, Français arts langagiers – immersion, 12e année (40S)* évalue les compétences des élèves dans deux domaines :

- La compréhension;
- L'écriture.

Le présent document traite de la compréhension. Il présente les modalités de correction dont la personne correctrice doit tenir compte afin de faire une évaluation juste et équitable des réponses des élèves.

Dans ce document vous trouverez :

- les modalités de correction;
- les apprentissages faisant l'objet de l'évaluation;
- les critères d'évaluation pour les tâches de compréhension;
- les tâches de compréhension et des pistes de réponses possibles;
- le tableau pour transposer la note de l'élève.

Modalités de correction

L'application des modalités de correction repose sur une bonne connaissance des apprentissages, des textes retenus, des tâches, des directives, des pistes de réponses possibles ainsi que des modèles de réponses d'élèves.

Compilation des notes

Le domaine de Compréhension compte pour 50 % de la note du test. La note que l'élève obtiendra pour ce domaine doit être transposée sur 50 points au moyen du tableau à la fin du présent document.

Préparation à la correction

- Bien connaître les compétences, les composantes des compétences, les apprentissages et les indicateurs de développement présentés dans le présent document.
- Bien connaître les critères d'évaluation pour les tâches de compréhension.
- Relire les textes qui se trouvent dans le *Cahier de préparation*.
- Étudier le présent document afin de bien comprendre les tâches de compréhension, les directives et les pistes de réponses possibles.
- Tenir compte du fait que l'évaluation de la compréhension vise surtout le contenu et l'organisation de la réponse de l'élève.

Cas particuliers relevés durant la correction

- ***Sources non indiquées*** – Lorsque l'élève n'indique pas une ou plusieurs de ses sources, la personne correctrice doit indiquer dans le cahier d'où provient le passage emprunté et attribuer une note uniquement pour la partie du travail qui appartient à l'élève.
- ***Réponses dans la même catégorie*** – Lorsque l'élève répond à deux questions dans la même catégorie, la personne correctrice doit corriger seulement la première réponse (tâche 1 ou 3). Il faut accorder la note zéro pour la deuxième catégorie.
- ***Réponses aux deux questions dans les deux catégories*** – Lorsque l'élève répond aux deux questions dans les deux catégories, la personne correctrice doit corriger seulement les premières réponses (tâches 1 et 3).
- ***Pas de réponse*** – Dans le cas d'un élève qui n'a pas fourni de réponse, il faut accorder la note zéro.
- ***Mots anglais ou anglicismes dans la réponse*** – Étant donné que cette partie du test porte sur la compréhension, l'élève qui, à l'occasion, utilise des mots anglais ou des anglicismes ne sera pas pénalisé pourvu que la réponse soit claire. Cependant, dans un cas extrême où la réponse est écrite plutôt en anglais, il faut accorder la note zéro.
- ***Réponse illisible*** – Lorsque l'écriture est indéchiffrable, il faut accorder la note zéro.

Les divisions scolaires ont désigné une personne coordonnatrice responsable de gérer la correction locale. Toute irrégularité (plagiat ou tricherie) doit être portée à l'attention de la personne coordonnatrice.

Si la personne correctrice éprouve de la difficulté à évaluer une réponse, elle doit consulter la personne coordonnatrice.

Dans le cas d'une demande de révision de note, la personne correctrice doit consulter la personne coordonnatrice qui se chargera de coordonner les séances de révision de note.

Apprentissages

Les apprentissages faisant l'objet de l'évaluation en compréhension sont présentés dans le tableau ci-dessous. Ce tableau reprend l'information présentée dans le schéma des apprentissages pour le stade *Autonome*[1]. Les textes choisis, ainsi que les tâches de compréhension, correspondent aux compétences, aux composantes des compétences et aux apprentissages incontournables de la 12e année retenus pour le test.

Dans la marge de droite de la clé de correction, en plus de la pondération accordée à chaque tâche, vous trouverez un code qui précise les composantes des compétences et les apprentissages visés. La lecture des codes se fait à l'aide du tableau suivant.[1]

11e et 12e années (AUTONOME)	
Penser et se construire **L'invention de soi se fait en interrogeant son propre langage pour le contrôler, l'ajuster et l'inventer à nouveau.**	
ÉCOUTER – VISIONNER – LIRE	**PARLER – REPRÉSENTER – ÉCRIRE**
L'ÉLÈVE DÉGAGE ET NÉGOCIE LE SENS DES IDÉES ET DE L'INFORMATION.	**L'ÉLÈVE S'EXPRIME SELON SON INTENTION, LE CONTEXTE ET LE DESTINATAIRE.**
L'élève cerne les éléments langagiers, les genres, les structures et les procédés dans les textes*. s **AÉV1, ALV1** Dégager des éléments constitutifs selon le genre de texte : – les éléments de la forme du genre; – les éléments qui créent des effets de vraisemblance, de suspense, d'exagération ou de rebondissement; – les éléments d'un film ou d'une pièce de théâtre tels que l'intrigue, le cadre, le décor, les costumes, le dialogue, les personnages, les procédés cinématographiques et les thèmes; – les éléments des documents médiatiques, analytiques, argumentatifs et de propagande tels que l'exposé d'une problématique, la présentation de ses composantes et l'ordre de ses composantes.	**L'élève s'exprime avec aisance et précision.** *(les habiletés fondatrices, les éléments langagiers – grammaire, vocabulaire, etc. – les genres, les structures, les procédés)* s **AP1** Respecter les conventions de communication : – le rythme, l'accent tonique, l'intonation; – la prononciation, l'articulation; – le débit; – le volume selon la situation de communication. s **ARÉ1** Respecter les conventions de communication : – la structure appropriée du texte; – la ponctuation et la majuscule. s **AP2, ARÉ2** Respecter les règles de la langue : – l'orthographe grammaticale : l'accord en genre et en nombre, la conjugaison; – la sémantique : le choix de termes, les interférences langagières; – la syntaxe : l'ordre des mots dans la phrase; – l'emploi correct des pronoms possessifs et démonstratifs; – l'orthographe d'usage (Écrire); – l'élision, la liaison (Parler). s **AP3, ARÉ3** Prévoir des procédés selon les conventions de communication orale et écrite et selon le message et le genre de texte (narratif, dialogal, poétique, descriptif, analytique, argumentatif, multimodal) : – des procédés qui appuient la communication orale : le champ lexical, le registre de langue, l'organisation des idées, les règles de la conversation, le langage non verbal, les éléments de la prosodie; – des procédés qui appuient la communication écrite : les procédés d'énonciation, lexicaux, syntaxiques et grammaticaux, stylistiques, sonores, graphiques, cinématographiques, de tonalité.

* Toutes présentations et représentations orales et écrites

1. MANITOBA, MINISTÈRE DE L'ÉDUCATION et de l'Apprentissage de la petite enfance, « Les apprentissages : l'explication de la lecture du tableau », Programme d'études : cadre curriculaire, Français arts langagiers – immersion, 11e et 12e années (Autonome), <https://www.edu.gov.mb.ca/m12/frpub/ped/fl2/cadre_9-12/index.html> (Consulté 19 avril 2023).

L'élève dégage le sens des propos et des textes*.
(les messages explicites et implicites, les compétences translinguistiques et culturelles)

- **AÉV2, ALV2** Comprendre des textes imaginaires et en délibérer :
  - reconnaître le sens des mots et la valeur qu'ils donnent au texte;
  - analyser le thème, le message et les valeurs véhiculées;
  - analyser les relations entre diverses composantes telles que les images, les thèmes, les personnages, les valeurs, le cadre, le temps de narration et le point de vue de narration;
  - analyser les caractéristiques physiques et psychologiques des personnages et les rapports qu'ils entretiennent;
  - analyser l'adaptation, au cinéma ou en bande dessinée, d'une œuvre littéraire;
  - analyser l'utilisation de la langue, y compris les figures de style, et des référents culturels pour évaluer l'effet créé.

- **AÉV3, ALV3** Comprendre des textes courants et en délibérer :
  - reconnaître le sens des mots et la valeur qu'ils donnent au texte;
  - analyser le thème, le message et les valeurs véhiculées;
  - distinguer les faits, les opinions, les hypothèses pour en évaluer l'objectivité et la subjectivité;
  - analyser les enjeux éthiques et sociaux pour comparer, au niveau du contenu et de la forme, les façons de traiter une même problématique;
  - analyser l'utilisation de la langue, y compris les figures de style, et des référents culturels pour communiquer un message.

- **AÉV4, ALV4** Dégager l'intention de l'auteur :
  - distinguer les procédés par lesquels l'auteur crée des effets dans le but d'exprimer son point de vue, de véhiculer son message ou de transmettre sa vision du monde;
  - analyser les techniques cinématographiques ou sonores utilisées pour mettre en relief les effets désirés et les valeurs véhiculées;
  - analyser l'impact des effets créés (le pouvoir lié à l'utilisation de la langue et aux éléments visuels et sonores).

L'élève se prononce de façon cohérente et respectueuse par rapport au fond en manipulant la forme.
(le choix d'une voix et la gestion de la voix des autres, le développement des idées, les compétences translinguistiques et culturelles)

- **AP4, ARÉ4** Établir sa voix en tenant compte de son intention de communication, du contexte, du destinataire et des enjeux sociaux et éthiques.

- **AP5, ARÉ5** Respecter les éléments de la cohérence : l'organisation et la progression des idées, les procédés lexicaux et les temps et modes verbaux.

- **AP6, ARÉ6** Formuler une synthèse des idées et de l'information.

- **AP7, ARÉ7** Créer une variété de textes* pour exprimer son imaginaire et sa vision du monde :
  - intégrer des procédés qui créent des effets;
  - mettre en œuvre la structure des schémas narratifs;
  - faire évoluer les personnages en tenant compte de leur rôle et importance, leurs actions et réactions, leur caractérisation et leur psychologie;
  - mettre en œuvre divers points de vue du narrateur (omniscient, témoin, participant);
  - intégrer des éléments de temps et de lieu;
  - évoquer des émotions, des sentiments et des réactions qui dévoilent sa vision du monde;
  - jouer avec la langue (y compris l'intégration des expressions idiomatiques et figées) pour créer des effets : s'amuser, se divertir, dramatiser, improviser, inciter.

- **AP8, ARÉ8** Créer une variété de textes* reliés aux thèmes complexes portant sur des enjeux sociaux ou éthiques ou des questions essentielles pour s'exprimer, informer, décrire, expliquer, analyser ou convaincre :
  - formuler un point de vue qui tient compte de diverses prises de position;
  - élaborer des idées pour développer une argumentation ou une analyse;
  - intégrer des procédés qui étayent ses arguments ou son analyse;
  - jouer avec la langue (y compris l'intégration des expressions idiomatiques et figées) pour créer des effets : s'amuser, se divertir, dramatiser, improviser, inciter;
  - s'appuyer sur des preuves pertinentes et crédibles.

* Toutes présentations et représentations orales et écrites

L'élève examine son point de vue, ses valeurs et ses sentiments par rapport aux messages des autres. s **AÉV5, ALV5** Analyser la portée du message et de ses éléments par rapport à soi-même : – examiner les émotions, les sentiments ou les réactions évoqués en soi ou l'impact des valeurs véhiculées par les textes exploités.	**L'élève exprime son point de vue, ses valeurs, ses sentiments et sa vision du monde.** s **AP9, ARÉ9** Communiquer et justifier son point de vue, ses sentiments, ses émotions et ses aspirations en intégrant un champ lexical précis.
L'élève soutient le bien-fondé de ce qui est dit pour faire évoluer ses pensées. s **AÉV6, ALV6** Soutenir le bien-fondé des textes imaginaires et courants : – poser des questions critiques, pertinentes et nuancées sur des sujets controversés, complexes ou abstraits; – justifier son interprétation à l'égard des sujets controversés, complexes ou abstraits; – développer son argumentation ou son analyse basée sur des preuves.	**L'élève se situe par rapport à la rétroaction des autres pour faire évoluer ses pensées.** s **AP10, ARÉ10** Enrichir son message en tenant compte des délibérations (des idées, des réactions et des rétroactions) entretenues avec ses pairs, son enseignant ou son public. s **AP11, ARÉ11** S'assurer de la pertinence et de la qualité de ses idées et de l'information intégrée dans ses textes* en fonction de son intention de communication et du sujet à traiter.

* Toutes présentations et représentations orales et écrites

Critères d'évaluation pour les tâches de Compréhension

Apprentissages **Lire, Visionner, Écrire**	**5**	**4**	**3**	**2**	**1**	**0**
La compréhension : 1 - Respect de l'intention de communication 2 - Élaboration de la compréhension 3 - Inclusion d'informations et de références qui appuient et font progresser les idées	Le texte respecte précisément l'intention de communication. L'explication est réfléchie et exprime en profondeur des idées pertinentes. Les informations et les références soutiennent et renforcent adroitement la progression des idées.	Le texte respecte très bien l'intention de communication. L'explication est claire et contient des idées détaillées. Les informations et les références sont bien choisies et assurent une progression appropriée des idées.	Le texte respecte généralement l'intention de communication. L'explication est adéquate et contient des idées générales. Les informations et les références sont adéquates et permettent une certaine progression des idées.	Le texte respecte partiellement l'intention de communication. L'explication est limitée et contient des idées superficielles. Les informations et les références sont peu nombreuses, insuffisantes, ou nuisent à la progression des idées.	Le texte respecte à peine l'intention de communication. La réponse est vague. Les informations et les références sont imprécises, voire erronées.	Non-respect de la tâche OU Manque évident de compréhension de la tâche. OU Absence de référence aux textes, au document visuel ou au document audiovisuel, selon le cas

	3	**2**	**1**	**0**
La cohérence : 1 - Organisation des idées et construction de paragraphes (organisateurs textuels) 2 - Harmonisation des temps verbaux	Le texte est bien organisé : les idées sont exprimées de façon claire et bien enchainée. L'harmonisation des temps verbaux est précise.	Le texte est organisé de façon adéquate : les idées sont exprimées de façon progressive. L'harmonisation des temps verbaux est appropriée.	Le texte est peu organisé : les idées sont exprimées de façon simpliste. L'harmonisation des temps verbaux est limitée.	Le texte manque d'organisation : les idées sont exprimées de façon inachevée. L'harmonisation des temps verbaux est rudimentaire.

	2	**1**	**0**
Les règles de la langue : 1 – Emploi des formes grammaticales 2 – Emploi du vocabulaire 3 – Emploi des structures syntaxiques 4 – Orthographe d'usage	La qualité de la langue est bonne et permet une expression efficace. Les formes grammaticales sont souvent correctes. Le vocabulaire est varié. Certaines structures syntaxiques sont efficaces. L'orthographe est souvent correcte.	La qualité de la langue est limitée malgré de nombreuses impropriétés. La grammaire est souvent inexacte. Le vocabulaire est limité. Plusieurs structures syntaxiques sont incorrectes. L'orthographe est parfois correcte.	La qualité de la langue est très limitée, voire incompréhensible. Il y a de nombreuses erreurs fondamentales de grammaire. Le vocabulaire est insuffisant. Le plupart des structures syntaxiques sont incorrectes. L'orthographe est rarement correcte.

Codes et pondération de chaque tâche :

Tâches et réponses

Les réponses fournies dans le présent document sont des pistes pour guider la correction. Quoique plusieurs exemples soient offerts, il est impossible de prévoir toutes les réponses acceptables. Ainsi, la personne correctrice est parfois appelée à porter un jugement professionnel sur la qualité de la réponse de l'élève.

Stimulus écrit : Rien à cacher

1. Dans la nouvelle « Rien à cacher », Natacha Spindelvev essaie de persuader le personnage principal, Ramzi Alkantara, à participer à ses recherches.

   Quels sont les dangers d'accepter la surveillance?

   Expliquez votre réponse en faisant référence à la nouvelle et à au moins un autre document du *Cahier de préparation*.

Des pistes pour des réponses :

AÉV3
ALV1
ALV2
ARÉ1
ARÉ2
ARÉ5
ARÉ6
ARÉ8

10 points

La nouvelle « Rien à cacher »

- **Dans la nouvelle, Natacha, membre de l'organisme IRSOT, fait une proposition à Ramzi. Étant donné qu'il est en situation de besoin, il permet à l'IRSOT de le surveiller pour que l'organisme puisse perfectionner le système de surveillance contre les terroristes. Il est séduit par les bénéfices du contrat.**

  – « Naturellement, si vous acceptez, vous serez rémunéré. Je sais que votre situation financière n'est pas des plus… des plus fastes, disons. » (lignes 179 – 180)

  En acceptant de se faire surveiller, il n'a plus de contrôle et devient victime des circonstances : des failles dans le système de surveillance.

  – « Obligation de me rendre dans leurs bureaux pour une entrevue, faute de quoi il me faudrait rembourser l'intégralité des sommes qui m'avaient été allouées. » (lignes 300 – 302)

  Bref, il perd son indépendance.

- **On doit questionner tout de suite la nature anodine de l'expérience, car l'organisme voulait un « type méditerranéen » (ligne 126), ce qui suggère des préjugées basées sur des stéréotypes. Bien que Ramzi saisisse ce stéréotype, il accepte :**

  – « Nous y voilà! Le type méditerranéen! On ne peut pas mieux tomber pour un profil de terroriste, pas vrai? Et comme je m'appelle Alkantara au lieu de Dupont ou Durand, l'affaire est bouclée! Ça fait de moi un poseur de bombes en puissance! » (lignes 127 – 130)

(suite à la page 8)

Codes et pondération de chaque tâche :

À cause d'une série de mésinterprétations du système de reconnaissance faciale, Ramzi est coincé et commence à ressembler au stéréotype noté au début de la nouvelle.

– « Résultat : je suis un pestiféré qu'on évite, devant lequel on s'empresse de changer de trottoir. Je me suis laissé pousser la barbe, c'était pire encore : avec mon teint mat et mon air sombre, on me prenait pour un barbu fanatique. » (lignes 445 – 448)

– « … j'attends que la rage qui me ronge en dedans soit devenue assez forte. J'attends le bon moment pour exploser… Comme une bombe HUMAINE. » (lignes 479 – 482)

- **À cause d'une faille dans le système et son absence lors d'une réunion imposée, Ramzi est accusé vers la fin de la nouvelle de manifester certaines émotions faciales et certains mouvements « anormaux » qui suggèrent des tendances agressives et potentiellement dangereuses pour la société. Bref, sa vie est en ruines faute d'une incapacité du système de reconnaissance faciale d'interpréter l'essence des émotions à partir des micro-expressions.**

  – « Ce vendredi, suite à votre passage dans la station de métro qui vous est habituelle, notre logiciel a détecté chez vous un ensemble de micro-expressions qui nous interroge. » (lignes 345 - 347)

  – « Nous avons pu établir une cartographie précise des émotions que dévoilent les signaux extrêmement rapides et fugaces que montre inconsciemment notre visage… » (lignes 349 - 351)

  – « Ce vendredi, donc, les microsignes perceptibles sur votre visage se sont révélés de même nature que ceux que nous avons pu constater chez des personnes qui nous intéressent au plus haut point. … celui des kamikazes, les bombes humaines, en phase de préaction. » (lignes 359 - 363)

  Malgré l'explication de Ramzi par rapport à ses émotions suite à la découverte de la situation médicale urgente de son père, il ne pouvait pas raisonner contre le système de reconnaissance faciale créé pour détecter des terroristes potentiels.

  – « Je venais d'apprendre que mon père sortait d'une série d'examens médicaux, les résultats n'étaient pas bons, très mauvais même. … Alors, oui, ce jour-là, j'avais les boules. » (lignes 384 - 389)

  À cause de cette interprétation fautive du système de surveillance, Ramzi est rejeté du programme, accusé d'être un danger pour la société, dépourvu des sommes allouées pour le projet et de la possibilité de suivre une vie normale. Tout lui est désormais interdit : les visites au restaurant, les cours universitaires, l'accès au bureau de poste, au supermarché, à la banque et au cinéma. Il ne peut même pas trouver un emploi.

  – « Désormais, je n'ai pas d'autre endroit où me rendre pour voir du monde, je suis en quarantaine. … Tout lieu public muni d'une caméra et d'un de ces foutus logiciels de reconnaissance faciale qui se répandent comme la peste m'est devenu interdit… .» (lignes 422 – 434)

  – « … quand ma tête apparaît dans un fichier d'offres d'emploi, plus un seul job n'est disponible pour moi. Alors, je vivote avec le minimum social qu'on accorde aux types de mon espèce pour qu'ils se tiennent tranquilles et que le système continue à tourner sans à-coups. » (lignes 456 – 460)

Codes et pondération de chaque tâche :

Les dangers reliés à la surveillance sont affichés dans plusieurs documents du *Cahier de préparation* :

Secrets d'enquête

- **Sous l'astuce #3, nous pouvons facilement considérer les dangers reliés à nos activités sur des réseaux sociaux. Nous ne reconnaissons souvent pas la capacité des hackers à surveiller ce que nous partageons avec des amis et de la famille dans le but de s'en servir pour des raisons malsaines.**
  - Les images avec « un faux Tom Cruise » ou du pape.
    - « Attention! Les images, les vidéos et les enregistrements sonores peuvent être manipulés. La vigilance est de mise. » (§ 58)
    - « Des milliers de photos d'une personne sont analysées par un programme… pour ensuite modifier des visages sur des vidéos. » (§ 60)

TikTok, ennemi public numéro 1

- Sous « Quel est le problème avec TikTok? », nous comprenons que les informations personnelles des utilisateurs de TikTok sont entreposées chez la multinationale ByteDance. Cette multinationale « est soumise à l'autorité du gouvernement communiste de Pékin, qui a tout pouvoir quand la sécurité du pays lui semble compromise. » (§ 3)

  Comme Ramzi, nous pouvons facilement croire que des réseaux n'existent que pour des raisons sincères et qu'il n'y aura pas de conséquences quand nous y participons, mais cela peut tourner mal si tout d'un coup un gouvernement décide de réclamer ces informations personnelles pour des raisons malsaines.
  - « … l'État chinois peut obliger ByteDance à transmettre les données personnelles des internautes aux services de renseignement ou à la police. » (§ 3)
  - « … le réseau compte aussi beaucoup d'adultes. Ils travaillent dans les administrations, les entreprises, les médias. Et ce sont leurs données personnelles qui sont considérées comme sensibles par les États. » (§ 4)

- Sous « La Chine espionne-t-elle vraiment tout le monde? », la légende sous l'image encerclée dévoile que « La surveillance se vit au quotidien en Chine : des millions de caméras à reconnaissance faciale sont là pour dénoncer les auteurs d'infractions mineures. » (§ 10) À cause des « infractions mineures » (§ 10), des individus ont leur visage affiché pour que tout le public puisse les identifier. Les conséquences : l'abandon de la part des amis ou de la famille, la perte d'emploi, les regards accusateurs. Les individus sont condamnés sur la place publique à cause de ces « infractions mineures » (§ 10) sans avoir l'occasion d'expliquer les circonstances ou les fausses interprétations de ce qui a été capté par la surveillance.

(suite à la page 10)

Codes et pondération de chaque tâche :

- Sous « La Chine espionne-t-elle vraiment tout le monde? », nous remarquons que des gouvernements et la multinationale ByteDance peuvent se servir des informations captées pour contrôler les critiques de leurs actions. Il est facile d'imaginer que des personnes puissent soudainement se faire accuser des actes contre ces gouvernements et multinationales s'ils décident qu'il s'agit d'une menace. Et une loi existe qui leur permet d'avoir accès aux informations s'ils croient que c'est nécessaire.
  - « ByteDance… a reconnu qu'une de ces équipes avait surveillé des journalistes américains qui enquêtaient sur elle! » (§ 5)
  - « … une loi datant de 2017 l'autorise à le faire s'ils estiment que sa sécurité nationale est en danger… » (§ 5)

- Sous « La Chine espionne-t-elle vraiment tout le monde? », nous découvrons que l'application TikTok est « un cheval de Troie » (§ 6) c'est-à-dire qu'elle « pourrait alors déclencher les caméras, les micros ou lire les messages. » (§ 6) À cause du fait que nous avons accepté les conditions de l'application, nous invitons la possibilité réelle de nous faire surveiller. TikTok devient le « parfait attirail pour surveiller les gouvernements ou dérober les secrets industriels des entreprises. » (§ 6) Bref, les dangers sont énormes.

- Sous « TikTok manipule-t-il les esprits? », nous nous rendons compte de l'efficacité de TikTok à inciter certains comportements. L'application est construite pour nous bercer; nous passons d'une vidéo à l'autre sans remarquer le temps qui passe. De plus, nous soupçonnons que l'algorithme nous dirige vers des informations qui reflètent les intérêts de la Chine.
  - « L'algorithme est-il programmé pour recommander des lectures conformes aux intérêts de la Chine? Nul ne le sait… » (§ 15)

  Alors, nous subissons bien probablement des stratégies pour manipuler notre pensée et nos croyances; c'est une conséquence de la permission que nous donnons à l'application.

Un vol d'identité aux répercussions

- **Nous nous attendons à ce que les banques aient des systèmes de sécurité en ligne pour nous protéger au cas où il y aurait des hackers qui surveillent notre activité bancaire. Si nous accordons trop de permission aux banques ou si nous ne sommes pas attentifs, nous pourrons être ciblés.**
  - Marie-Chantal Perron a découvert que son identité avait été volée à partir de certaines transactions avec sa carte de crédit.
    - « Quand j'ai voulu déclarer la fraude, on m'a signalé qu'il n'y avait rien d'anormal dans ces deux transactions financières, car elles avaient été validées avec mes renseignements personnels. La banque avait appelé mon numéro et je leur avais renseigné mon nom, mon adresse et ma date de naissance, ce qui était bien évidemment faux. » (§ 4)

Il fallait attendre neuf mois avant que cette situation ne soit réglée.

- « Dans les cas d'un vol d'identité numérique, je trouve cela ridicule que le gouvernement ne fasse pas preuve de collaboration et de rapidité. J'ai pu seulement toucher cette aide financière en février 2022. Les enjeux de la cybercriminalité ne sont pas encore compris par nos dirigeants politiques », regrette Marie-Chantal Perron. » (§ 10)

Menace sur la cybersécurité

- **L'image de la caméra à la page 45 nous donne un sens de sécurité; elle nous surveille pour nous protéger. Cependant, cette caméra peut subir une attaque, ce qui nous rend aussi vulnérables.**
  - « La défaillance du logiciel qui contrôle une caméra de surveillance peut la rendre vulnérable à une attaque. Son usage est alors détourné et ses données piratées. » (§ 15)

Tiré du document audiovisuel

- **Baptiste Robert nous conseille de nous méfier de nos montres connectées, qui permettent à certains logiciels de nous surveiller. Il constate que nous devrions limiter accès aux informations personnelles pour nous protéger.**
  - **Mouloud :** Est-ce que c'est bien d'avoir une montre connectée? Est-ce que ça donne aussi, est-ce qu'on peut bloquer les infos qu'on donne, moi sur mon téléphone, nous tous, est-ce qu'on a un moyen de bloquer les infos qu'on donne? (08:12)
  - **Baptiste Robert :** Alors, oui parce que principalement que ce soit sur les deux grandes marques de téléphone, vous avez un système de permission et donc, vous avez une granularité qui est assez importante et vous pouvez dire, par exemple, je ne veux pas que cette application utilise le microphone, je ne veux pas que cette application utilise le GPS. […] Après le reste, vous faites vos choix. (08:19)

- **Les témoignages suggèrent que les réseaux sociaux nous surveillent. Alors, les dangers que nous imaginons sont réels. Il faut toujours être attentif si nous souhaitons nous protéger de la surveillance des autres.**
  - **Mark Zuckerberg, créateur de Facebook :** « Vous parlez de cette théorie du complot qui voudrait que nous écoutions ce que vous dites sur votre téléphone pour faire de la publicité. Nous ne faisons pas ça! » (02:59)
  - **Narratrice :** Des lanceurs d'alerte avancent que tous ces micros nous enregistrent bel et bien pour perfectionner leurs algorithmes. (03:13)
  - **Thomas Le Bonniec (ancien analyste de données – sous-traitant Apple) :** Dans les enregistrements on entendait toutes sortes de choses. On entendait des numéros de téléphone, on entendait des noms propres, on entendait des choses extrêmement intimes. (03:18)

(suite à la page 12)

Codes et pondération de chaque tâche :

- **« Nous sommes naïfs à l'égard des dangers, ce qui peut mettre notre sécurité en péril. Nous offrons trop d'informations parce que nous croyons que la politesse l'exige », explique Baptiste Robert (05:50). Même si le téléphone « ne va pas ouvrir le micro sans… autorisation »,**

  – « on est très très gentil, on lui donne beaucoup, beaucoup de données donc en fait, quand vous utilisez votre téléphone, quand vous utilisez TikTok par exemple, vous n'envoyez pas qu'une vidéo, vous envoyez plein de données autour. »

Codes et pondération de chaque tâche :

Stimulus visuel : L'image « Votre empreinte numérique »

2. L'image « Votre empreinte numérique est plus importante que vous ne le pensez » représente visuellement des aspects reliés au thème.

   Comment cette image reflète-t-elle le thème *L'empreinte numérique : rêve ou cauchemar?*

   Élaborez votre réponse en faisant référence aux images et aux informations tirées d'au moins deux documents du *Cahier de préparation*.

Des pistes pour des réponses :

ALV2
ARÉ2
ARÉ5
ARÉ6
ARÉ8

10 points

L'image « Votre empreinte numérique est plus importante que vous ne le pensez »

- **Cette image évoque :**
  - le rêve de pouvoir afficher des informations sur des réseaux sans soucis, car des gens comme des hackers éthiques, représentés par le personnage avec la loupe, guettent toute action qui pourrait nous menacer. Alors, le personnage assis devant l'ordinateur peut explorer les réseaux et les sites sans peur. Même l'éclairage jaunâtre et ensoleillé suggère que les hackers éthiques voient clairement et peuvent éloigner tout danger.
  - le cauchemar, car l'interprétation peut être complètement inversée. Le personnage avec la loupe, qui indique le danger, espionne le personnage assis devant l'ordinateur. Ce personnage ignore l'omniprésence du danger, des hackers mal intentionnés qui cherchent à voler des informations personnelles des gens qui ne se soupçonnent de rien.

Dans l'article « Secrets d'enquête »

- **Sous l'astuce #3, le rêve et le cauchemar sont évidents. Nous nous attendons à ce que la véracité soit affichée sur des sites web. Malheureusement ces informations peuvent être fausses. En y croyant et en répétant ce que nous voyons ou lisons, nous nous mettons possiblement dans une situation précaire ou humiliante.**
  - Les images avec « un faux Tom Cruise » ou du pape.
    - « Attention! Les images, les vidéos et les enregistrements sonores peuvent être manipulés. La vigilance est de mise. » (§ 58)
    - « Lorsqu'on prête attention, on peut détecter qu'il s'agit d'un montage » (§ 59)
    - « Des milliers de photos d'une personne sont analysées par un programme… pour ensuite modifier des visages sur des vidéos. » (§ 60)

(suite à la page 14)

Codes et pondération de chaque tâche :

L'article « Menace sur la cybersécurité »

- **L'image de la caméra à la page 45 peut nous donner un sens de sécurité; cela nous protège (le rêve). Cependant, cette caméra avec du rouge en arrière-plan pourrait aussi signaler un cauchemar.**
  - « La défaillance du logiciel qui contrôle une caméra de surveillance peut la rendre vulnérable à une attaque. Son usage est alors détourné et ses données piratées. » (§ 15)

- **L'image du BOT à la page 46 évoque des cauchemars. Bien que nous nous servions de l'ordinateur en croyant que nous le faisons en toute sécurité (le rêve), certains utilisent des techniques qui visent usurper notre identité ou nos biens.**
  - « Des experts en sûreté et en sécurité travaillent au quotidien pour que notre navigation et nos échanges se déroulent avec une transmission fiable d'informations, autour de dispositifs capables de résister à une action malveillante. » (§ 19)
  - « Les techniques qui nous piègent : Le hameçonnage (ou le phishing)… typosquattage… vol de mot de passe… un virus informatique… les rançongiciels… la modification de données… au blocage de la transmission d'informations… » (§ 20-25)

TikTok, ennemi public numéro 1

- **Dans le texte, « Quel est le problème avec TikTok? », la photo du P.D.-G de TikTok, qui « a essayé de rassurer le Congrès américain sur l'indépendance de l'application par rapport au gouvernement chinois » (§ A) paraît souriant et sincère. Les gens peuvent se servir de TikTok sans aucun souci. Malgré les assurances que TikTok est une application qui permet aux utilisateurs de l'explorer sans peur, le cauchemar est très évident selon les informations qui accompagnent l'image.**
  - « … l'État chinois peut obliger ByteDance à transmettre les données personnelles des internautes aux services de renseignement ou à la police. » (§ 3)
  - « … le réseau compte aussi beaucoup d'adultes. Ils travaillent dans les administrations, les entreprises, les médias. Et ce sont leurs données personnelles qui sont considérées comme sensibles par les États. » (§ 4)

- **Le personnage qui ressemble à Captain America dans l'image subit des attaques d'une multitude de logos TikTok. En regardant les logos TikTok de façon séparée, nous dirions que cela ressemble à des notes de musique ou des décorations; c'est une célébration destinée aux multiples utilisateurs de TikTok.**
  - « … le réseau social a une audience considérable avec 1,2 milliard d'utilisateurs actifs mensuels. » (« Quel est le problème avec TikTok? », § 4)

Pourtant, le cauchemar se voit en considérant toute l'image. Captain America fait son possible de se protéger et de protéger les citoyens américains (représentés par le drapeau) contre le bombardement continu de TikTok. Nous imaginons facilement que TikTok souhaite envahir des lieux protégés, que cela soit les citoyens des États-Unis ou notre empreinte numérique. Cette interprétation cauchemardesque de l'image et du thème s'appuie de plusieurs faits :

– « ByteDance… a reconnu qu'une de ses équipes avait surveillé des journalistes américains qui enquêtaient sur elle! » (« La Chine espionne-t-elle vraiment tout le monde? », § 5)

– « … une loi datant de 2017 l'autorise à le faire s'ils estiment que sa sécurité nationale est en danger… » (« La Chine espionne-t-elle vraiment tout le monde? », § 5)

– TikTok est « un cheval de Troie ». Il « pourrait alors déclencher les caméras, les micros ou lire les messages. » (« La Chine espionne-t-elle vraiment tout le monde? », § 6)

Nous soupçonnons que les attaques de la part de TikTok sont constantes; les algorithmes nous visent constamment.

– « L'algorithme est-il programmé pour recommander des lectures conformes aux intérêts de la Chine? Nul ne le sait… » (« TikTok manipule-t-il les esprits », § 15)

- **Le réve et le cauchemar se juxtaposent dans l'image encerclée agencée au texte, « La Chine espionne-t-elle vraiment tout le monde? ». La légende sous l'image dit : « La surveillance se vit au quotidien en Chine : des millions de caméras à reconnaissance faciale sont là pour dénoncer les auteurs d'infractions mineures ». (§ 10) D'une part, nous pouvons remercier la présence des caméras qui nous surveillent pour garantir des quartiers sécuritaires. Mais les caméras ne peuvent nous assurer d'une bonne interprétation des actions enregistrées. Les individus accusés de certaines « infractions mineures » ont leur visage affiché en public et perdent l'occasion de se défendre contre l'accusation.**

(suite à la page 16)

Codes et pondération de chaque tâche :

Stimulus audiovisuel : Est-ce que nos téléphones nous écoutent

3. Dans le document audiovisuel, « Est-ce que nos téléphones nous écoutent? », il est question des problèmes associés à notre empreinte numérique.

   Selon vous, peut-on se protéger contre les dangers que pose l'empreinte numérique?

   Justifiez votre réponse en faisant référence aux informations tirées du document audiovisuel et d'au moins un autre document du *Cahier de préparation*.

Des pistes pour des réponses :

AÉV1
AÉV3
ALV3
ARÉ1
ARÉ3
ARÉ5
ARÉ6
ARÉ8
ARÉ9

Oui, on peut se protéger contre les dangers que pose l'empreinte numérique.
Le document audiovisuel

> Nous pouvons nous protéger des dangers de notre empreinte numérique en nous fiant aux hackers éthiques, en assurant le contrôle de nos informations et en nous renseignant sur les moyens utilisés pour voler nos données.

- **Bien que des dangers existent, nous pouvons nous fier au travail des hackers éthiques, qui veillent à ce que les failles de sécurité soient réglées. Alors, leur persévérance enlève des soucis face aux dangers.**

  – **Baptiste Robert :** (…) un hacker éthique c'est un hacker qui va utiliser ses compétences comme tous les hackers. Sauf qu'il va avoir l'éthique vraiment au centre de son action et va essayer entre guillemets d'utiliser ses compétences pour le bien commun. Donc, quand il veut trouver une faille de sécurité par exemple dans une application mobile dans une entreprise. Quand il trouve des données, il va essayer de contacter l'entreprise en question, les personnes concernées pour que l'entreprise protège un petit peu mieux ses données, ses utilisateurs et son application globale. (03:45)

- **En répondant à la question posée de la part de Mouloud, Baptiste Robert nous assure que nous avons la capacité de contrôler nos informations. Donc, nous nous protégeons en limitant accès à nos informations personnelles… notre empreinte numérique.**

  – **Mouloud :** Est-ce que c'est bien d'avoir une montre connectée? Est-ce que ça donne aussi, est-ce qu'on peut bloquer les infos qu'on donne, moi sur mon téléphone, nous tous, est-ce qu'on a un moyen de bloquer les infos qu'on donne? (08:12)

  – **Baptiste Robert :** Alors, oui parce que principalement, que ce soit sur les deux grandes marques de téléphone, vous avez un système de permission et donc, vous avez une granularité qui est assez importante et vous pouvez dire, par exemple, je ne veux pas que cette application utilise le microphone, je ne veux pas que cette application utilise le GPS. … Après le reste, vous faites vos choix. (08:19)

- **Grâce à la discussion avec le hacker éthique, Baptiste Robert, nous sommes bien outillés de « trucs » qui peuvent nous protéger. Les recommandations sont multiples :**
  - Refuser de mettre l'adresse courriel pour nous brancher au wifi d'un aéroport.
    - **Baptiste Robert :**… vous êtes à l'aéroport, vous vous connectez au wifi de l'aéroport, on vous demande une adresse email. Et en fait, pour accéder au wifi, vous n'avez pas besoin de l'e-mail fondamentalement et si vous mettez n'importe quoi, ça va quand même marcher. (09:34)
    - Yasine confirme : Vous mettez mail@mail, ça marche très bien. (09:59)
  - Créer et maintenir une fausse identité dans certaines situations.
    - **Baptiste Robert :** C'est un conseil que je donne souvent, c'est qu'il faut mentir et mentir régulièrement de manière consistante. C'est-à-dire qu'il faut se créer une identité : aujourd'hui, je m'appelle Baptiste Robert sur Internet. Demain je m'appelle John Doe, j'aurais un autre âge, après-demain je m'appellerais Jane Doe, je serais une femme et j'aurais encore un autre âge. C'est de mentir de manière constante, régulièrement. (10:15)
  - Utiliser deux adresses.
    - **Mouloud :** J'ai deux adresses pour ces choses-là moi… (10:35)

- **Grâce aux conseils du hacker éthique, Baptiste Robert, nous sommes bien informés des « petits jouets » des hackers. En nous informant de la technologie, nous nous protégeons des dangers.**
  - **Baptiste Robert :** On va avoir une première clé USB qui est une clé USB assez simple et en fait qui permet d'automatiser en gros le hacking. Typiquement, cette clé USB, elle a été utilisée dans une situation précise. (10:44)
    Cela a été utilisé pour télécharger des informations d'un ordi d'une guichetière d'une banque.
  - **Baptiste Robert :** (…) donc ça vous le voyez c'est un câble standard d'iPhone, mais en réalité en fait à l'intérieur ici là vous allez voir un circuit imprimé qui permet de contacter en fait à distance le téléphone qui va être branché au câble. Je laisse ça par exemple dans un endroit public, voilà vous allez brancher pour recharger votre téléphone et en fait je vais prendre le contrôle juste parce que vous avez branché. (12:40)
  - **Baptiste Robert :** Le troisième, en fait, c'est un petit objet qu'on peut se balader. En gros ça va être une bande wifi. En fait, cela va être ma bande wifi, donc je vais pouvoir, si vous vous connectez là-dessus… Donc je vais l'appeler, par exemple, Clique-Guest et donc vous allez vous connecter dessus et je vais pouvoir voir tout le trafic qui passe. Mais même sans vous connecter en fait, juste si je l'allume, je vais savoir tous les wifi qui sont enregistrés sur vos téléphones. (13:28)

(suite à la page 18)

Codes et pondération de chaque tâche :

Des documents du *Cahier de préparation*

- **Même si nous avons été trompés par un organisme malsain, nous pouvons nous fier à des agences pour nous secourir. Ces agences sont équipées de spécialistes pour répondre aux attaques.**

  Documents qui appuient cet élément de réponse

  – Le document « **En marche vers la justice** »
    - « Il existe plusieurs bureaux de cyberenquête au Canada. On en trouve à la Sûreté du Québec (SQ), à l'agence du revenu du Canada (ARC), à Sécurité publique Canada et même au ministère de l'Éducation. Ces équipes regroupent des spécialistes provenant de tous les horizons : enquêteurs, informaticiennes, journalistes, analystes de données, conseillères juridiques, agents de renseignements ou intervieweurs. » (§ 38)

  – Le document « **Menace sur la cybersécurité** » :
    - « Des experts en sûreté et en sécurité travaillent au quotidien pour que notre navigation et nos échanges se déroulent avec une transmission fiable d'informations, autour de dispositifs capables de résister à une action malveillante. » (§ 19)

- **Il existe beaucoup de suggestions que nous pouvons facilement mettre en vigueur pour nous protéger. Il suffit de les mettre en pratique.**

  – Le document « Un vol d'identité aux répercussions multiples » :
    - « Pour se protéger d'un vol d'identité, plusieurs conseils et solutions sont importants à connaître :
      - Consultez et contrôlez vos factures et relevés bancaires…
      - Optez pour une double authentification…
      - Détectez les signes de fraude ou de vol d'identité…
      - Créez des mots de passe complexes et uniques…
      - Évitez d'ouvrir et de cliquer sur des liens intégrés à des messages…
      - Limitez les informations et les photos que vous partagez…
      - Évitez de sauvegarder vos informations personnelles ou professionnelles sur votre navigateur…
      - Déchiquetez tous les documents physiques qui contiennent des informations personnelles…
      - Assurez-vous que votre système informatique soit muni d'un antivirus. » (§ 18 - § 26)

  – Le document « **Menace sur la cybersécurité** » nous informe du chiffrement, ce qui nous protège. De plus, les scientifiques sont toujours aux aguets pour inventer de nouvelles formes de chiffrement pour nous protéger.
    - « Le chiffrement permet non seulement de protéger des données contre un vol ou une menace, mais aussi de prouver que les informations sont authentiques. Il garantit que le message provient de la bonne personne et n'a pas été transformé. » (§ 26)

Codes et pondération de chaque tâche :

- « À la recherche du cryptage parfait, les scientifiques imaginent de nouvelles formes de chiffrement, tout en essayant d'anticiper au maximum les technologies informatiques du futur. » (§ 37)

Des pistes pour des réponses :

Non, on ne peut pas se protéger contre les dangers que pose l'empreinte numérique.
Le document audiovisuel

Étant donné notre attitude d'indifférence, notre ignorance en ce qui concerne les permissions à accorder ou non aux applications, de nature frauduleuse et innovatrice des organismes malsains et les moyens toujours plus originaux de nous tromper ou voler nos données, nous ne pouvons pas nous protéger des dangers reliés à notre empreinte numérique.

- **Les opinions des invités reflètent celles de la population. Certaines personnes s'inquiètent des dangers de l'empreinte numérique tandis que d'autres en sont moins perturbés.**
  - **Xavier :** Je pense qu'il y a des, des, peut-être partiellement, c'est selon les applis en vrai, ça on le sait. (0:50)
  - **Agnès :** Non j'suis pas parano, et je pense que oui il y a des trucs qui font que mon petit panier là, ils me suivent un peu tous! mais je pense pas qu'on m'écoute quoi! (01:00)

- **Malgré le fait que Mark Zuckerberg, créateur de Facebook, nous assure que l'on n'écoute pas à ce qui est dit au téléphone pour faire de la publicité, plusieurs en disent le contraire. Alors, on soupçonne fortement que ces réseaux nous guettent.**
  - **Mark Zuckerberg, créateur de Facebook :** « Vous parlez de cette théorie du complot qui voudrait que nous écoutions ce que vous dites sur votre téléphone pour faire de la publicité. Nous ne faisons pas ça! » (02:59)
  - **Narratrice :** Des lanceurs d'alerte avancent que tous ces micros nous enregistrent bel et bien pour perfectionner leurs algorithmes. (03:13)
  - **Thomas Le Bonniec (ancien analyste de données – sous-traitant Apple) :** Dans les enregistrements on entendait toutes sortes de choses. On entendait des numéros de téléphone, on entendait des noms propres, on entendait des choses extrêmement intimes. (03:18)

- **Même le gouvernement avec toutes les ressources disponibles ne peut se protéger. Alors, les gens ordinaires ne sont certainement pas équipés pour répondre aux attaques entraînées par l'appropriation de notre empreinte numérique.**

(suite à la page 20)

Codes et pondération de chaque tâche :

- En se référant à Baptiste Robert, Mouloud dit : (…) Vous avez repéré des failles de sécurité sur des sites et des applications qui appartenaient aux gouvernements français, indien et américain. (04:21). Robert Baptiste affirme : J'avais accès à tous les groupes de messagerie, j'avais accès aux contacts, j'avais accès voilà. (05:15)
- Baptiste Robert divulgue : J'ai beaucoup travaillé sur le cyberespace indien, donc j'ai trouvé une faille dans l'application du Premier ministre indien, par exemple, et alors ce qui était assez rigolo en fait, c'est que j'ai publié quelque chose sur Twitter relatif à ça et 30 secondes après, j'ai le bureau du Premier ministre qui m'a contacté. (11:57)

- **La nature humaine est telle que nous offrons trop d'information, et ce à cause de la politesse. Cette nature humaine nous met dans une situation précaire face aux organismes malsains qui nous guettent à travers l'empreinte numérique. Baptiste Robert cite plusieurs exemples de ceci (05:50). Même si le téléphone « ne va pas ouvrir le micro sans… autorisation »,**
  - « on est très très gentil, on lui donne beaucoup, beaucoup de données donc en fait, quand vous utilisez votre téléphone, quand vous utilisez TikTok par exemple, vous n'envoyez pas qu'une vidéo, vous envoyez plein de données autour. » (05:50)
  - le wifi allumé « va scanner tous les wifi aux alentours, et grâce au wifi, il va aussi être capable de vous localiser plus que votre téléphone. Il a bien le réseau, il est capable de savoir les antennes qu'il y a autour. Donc en fait il a tout un tas d'informations dans votre usage quotidien du téléphone qui vont être collectés, récoltés, stockés, analysés et recoupés par des géants. » (05:50)
  - « … il y a des métiers, il y a ce qu'on appelle des Data Brokers, donc des gens qui achètent de la donnée en masse et dont le métier c'est de prendre des milliards et des milliards de données de plein de côtés, de les regrouper ensemble pour faire des profils de personnes. (05:50)

- **Baptiste Robert dévoile des exemples d'outils ou de « trucs » à la fois simples et sophistiqués qui peuvent facilement nous tromper dans le but de voler des informations à notre sujet. Bien que nous soyons informés de cette technologie, nous ne pouvons pas réussir à nous protéger des dangers.**
  - **Baptiste Robert :** On va avoir une première clé USB qui est une clé USB assez simple et en fait qui permet d'automatiser en gros le hacking. Typiquement, cette clé USB, elle a été utilisée dans une situation précise. (10:44)
    Cela a été utilisé pour télécharger des informations d'un ordi d'une guichetière d'une banque.
  - **Baptiste Robert :** (…) donc ça vous le voyez c'est un câble standard d'iPhone, mais en réalité en fait à l'intérieur ici là vous allez voir un circuit imprimé qui permet de contacter en fait à distance le téléphone qui va être branché au câble. Je laisse ça par exemple dans un endroit public, voilà vous allez brancher pour recharger votre téléphone et en fait je vais prendre le contrôle juste parce que vous avez branché. (12:40)

– **Baptiste Robert :** Le troisième, en fait, c'est un petit objet qu'on peut se balader. En gros ça va être une bande wifi. En fait, cela va être ma bande wifi, donc je vais pouvoir, si vous vous connectez là-dessus… Donc je vais l'appeler, par exemple, Clique-Guest et donc vous allez vous connecter dessus et je vais pouvoir voir tout le trafic qui passe. Mais même sans vous connecter en fait, juste si je l'allume, je vais savoir tous les wifi qui sont enregistrés sur vos téléphones. (13:28)

Des documents du *Cahier de préparation*

TikTok, ennemi public numéro 1

- **Les réseaux sociaux sont très puissants. Les gouvernements qui devraient avoir le pouvoir de nous protéger sont impuissants à cause de l'espionnage calculé des autres gouvernements, et ce selon des applications pour lesquelles nous acceptons les conditions pour pouvoir nous en servir. Alors, nous pouvons facilement devenir victimes de notre empreinte numérique.**

  – Sous « Quel est le problème avec TikTok? », nous comprenons que les informations personnelles des utilisateurs de TikTok sont entreposées chez la multinationale ByteDance. Cette multinationale « est soumise à l'autorité du gouvernement communiste de Pékin, qui a tout pouvoir quand la sécurité du pays lui semble compromise. » (§ 3) La Chine « peut obliger ByteDance à transmettre les données personnelles des internautes aux services de renseignement ou à la police. » (§ 3)

- **« La Chine espionne-t-elle vraiment tout le monde? » nous dévoile que certains pays ont des lois qui leur permettent de nous surveiller s'ils se sentent menacés. Comment pourrions-nous lutter contre des lois qui permettent cette surveillance?**

  – « ByteDance… a reconnu qu'une de ces équipes avait surveillé des journalistes américains qui enquêtaient sur elle! » (§ 5)

  – « … une loi datant de 2017 l'autorise à le faire s'ils estiment que sa sécurité nationale est en danger… » (§ 5)

- **Sous « La Chine espionne-t-elle vraiment tout le monde? », nous apprenons qu'en acceptant les conditions de l'application pour pouvoir nous en servir, nous acceptons aussi les dangers. Il semble ne pas avoir des problèmes de sécurité pour nous protéger.**

  – TikTok est « un cheval de Troie », c'est-à-dire qu'elle « pourrait alors déclencher les caméras, les micros ou lire les messages. » (§ 6)

- **Si les gouvernements ne peuvent pas se protéger des dangers, les citoyens ont encore moins de chance de se protéger des dangers.**

  – TikTok devient le « parfait attirail pour surveiller les gouvernements ou dérober les secrets industriels des entreprises. » (§ 6)

(suite à la page 22)

Codes et pondération de chaque tâche :

- **Les gens qui croient qu'ils peuvent se protéger contre les dangers sont soit naïfs soit ignorants. La cybersécurité ne réussit aucunement à protéger leurs informations personnelles. Cette prise de position est confirmée dans « Est-il pire que les autres réseaux sociaux? »**

  – « De plus, la "cybersécurité" est insuffisante sur toutes les plateformes : des données privées fuitent régulièrement. En janvier, les adresses électroniques de 235 millions d'utilisateurs de Twitter ont ainsi été mises en vente sur un forum de "hackers!" » (§ 20)

Un vol d'identité aux répercussions multiples

- **La réalité est telle que notre empreinte numérique peut nous exposer à des dangers à cause des malfaiteurs qui peuvent y avoir accès. Il y a par la suite très peu d'appui du gouvernement pour résoudre la fuite d'information.**

  – Le document « **Un vol d'identité aux répercussions multiples** » : Marie-Chantal Perron a découvert que des transactions ont été effectuées sur sa carte de crédit sans son autorisation. En faisant l'appel pour signaler cette anormalité, elle a découvert que son identité avait été volée.

    ▫ « Quand j'ai voulu déclarer la fraude, on m'a signalé qu'il n'y avait rien d'anormal dans ces deux transactions financières, car elles avaient été validées avec mes renseignements personnels. La banque avait appelé mon numéro et je leur avais renseigné mon nom, mon adresse et ma date de naissance, ce qui était bien évidemment faux. » (§ 4)

  Le processus pour rectifier la situation a pris neuf mois.

    ▫ « Dans les cas d'un vol d'identité numérique, je trouve cela ridicule que le gouvernement ne fasse pas preuve de collaboration et de rapidité. J'ai pu seulement toucher cette aide financière en février 2022. Les enjeux de la cybercriminalité ne sont pas encore compris par nos dirigeants politiques », regrette Marie-Chantal Perron. » (§ 10)

Menace sur la cybersécurité

- **Nous ne sommes pas tous adeptes à éviter des pièges. Alors, nos faiblesses face à la sécurité numérique peuvent donner accès à notre empreinte numérique.**

  – Le document « **Menace sur la cybersécurité** » énumère toute une gamme de pièges à la page 46 :

    ▫ le hameçonnage (ou le phishing) (§ 20)
    ▫ les attaques de typosquattage (§ 20)
    ▫ le vol de mot de passe (§ 21)
    ▫ les botnets (§ 22)
    ▫ les rançongiciels (§ 24)
    ▫ la modification de données (§ 25)
    ▫ les usurpations d'identité. (§ 25)

Codes et pondération de chaque tâche :

Stimulus écrit : Menace sur la cybersécurité

4. Dans l'article, « Menace sur la cybersécurité », on nous rassure que « la sûreté et la sécurité de l'utilisation des réseaux sont une priorité pour les gouvernements, les entreprises et pour les concepteurs de logiciels et de sites Web » (p. 45)

   À votre avis, est-ce que la surveillance de notre empreinte numérique par les agences gouvernementales, bancaires et commerciales est justifiable?

   Justifiez votre réponse en faisant référence à des informations tirées de cet article et au document audiovisuel.

Des pistes pour des réponses :

AÉV1
AÉV3
ALV3
ARÉ1
ARÉ3
ARÉ5
ARÉ6
ARÉ8
ARÉ9

10 points

Oui, je suis d'accord. La surveillance de notre empreinte numérique par les agences gouvernementales, bancaires et commerciales est justifiable.

Dans le document « Menace sur la cybersécurité » :

- **Avec toutes les connexions à Internet (« smartphones, ordinateurs, systèmes d'alarme, voitures et maisons » (§ 1), les « systèmes sont parfois vulnérables aux attaques de pirates informatiques, qui veulent obtenir de précieuses données personnelles » (§ 1). Ce réseautage n'est pas limité aux ordinateurs. « C'est le cas de plus en plus de voitures, d'appareils de santé et même de nos réfrigérateurs! » (§ 6). Les agences peuvent certainement nous épauler, et ce pour nous protéger des conséquences réelles :**
  - « En 2012, 164 millions d'adresses informatiques et de mots de passe ont été extraits du site Linkedin, mais l'attaque n'a été découverte que 4 ans plus tard! » (§ 4)
  - « En 2014, des pirates informatiques ont dérobé l'équivalent de 450 millions de dollars au site Mt Gox sous forme de monnaie dématérialisée. » (§ 5)

- **« Selon le site Planetoscope.com, 29 000 gigaoctets d'informations sont publiés chaque seconde dans le monde. » (§ 12) Nous ne pouvons pas croire avec certitude que toutes ces informations passent sans être susceptibles aux attaques. Les agences doivent pouvoir intervenir pour nous assurer de la sécurité. Nous comprenons heureusement que « ces questions ont été prises au sérieux depuis très longtemps (…). À l'heure de l'informatique, la sûreté et la sécurité de l'utilisation des réseaux sont une priorité pour les gouvernements, les entreprises et pour les concepteurs de logiciels et de sites Web. » (§ 13)**

(suite à la page 24)

Codes et pondération de chaque tâche :

- **Pour tous ceux qui interagissent avec des réseaux, les concepteurs comme les utilisateurs, il y a un intérêt important pour la sécurité. Certaines agences sont bien équipées pour réaliser cette responsabilité.**
  - « Dans la masse d'informations qui circule sur le web, il est essentiel de garantir leur intégrité, leur confidentialité, et leur disponibilité à tout moment. Tout en s'assurant que seules les personnes autorisées ont accès aux ressources! » (§ 16)
  - « La sécurité informatique nécessite donc une approche globale d'un bout à l'autre de la chaîne. » (§ 17)

- **Étant donné le nombre de pièges qu'il faut éviter, les agences qui surveillent notre empreinte numérique contrebalancent nos faiblesses face à la sécurité. Ces pièges sont énumérés à la page 46 :**
  - l'hameçonnage (ou le phishing) (§ 20)
  - les attaques de typosquattage (§ 20)
  - le vol de mot de passe (§ 21)
  - les botnets (§ 22)
  - les rançongiciels (§ 24)
  - la modification de données (§ 25)
  - les usurpations d'identité. (§ 25)

- **Bien que certaines personnes disent que le chiffrement garantit « l'authenticité d'un message » (§ 29), il n'y a que certaines clés qui réussissent à nous protéger. Cette incertitude face à la sécurité selon le genre de clé utilisée souligne l'importance d'avoir des agences qui surveillent notre empreinte numérique, et ce pour notre bien-être.**
  - Les clés symétriques sont cependant plus faibles que les clés dites asymétriques. » (§ 30)

- **Le texte nous informe que « D'ici quelques années, l'apparition d'ordinateurs extrêmement rapides pourrait remettre en cause le cryptage actuel. La puissance des ordinateurs et des débits d'informations ne cesse d'augmenter… » (§ 37) À cause de cette évolution vertigineuse, ce serait la folie de ne pas vouloir l'intervention des agences pour garantir la sécurité de notre empreinte numérique.**

Dans le document audiovisuel :

La surveillance de la part des agences gouvernementales, bancaires et commerciales, nous donne un sens de sécurité. Nous faisons notre possible de détourner des attaques malsaines de la part des malfaiteurs et nous avons en plus l'appui de ces organismes.

Codes et pondération de chaque tâche :

- **Certains hackers éthiques travaillent avec des organismes pour dévoiler des failles de sécurité. Nous nous fions de leur persévérance à nous protéger.**
  - **Baptiste Robert :** (…) un hacker éthique c'est un hacker qui va utiliser ses compétences comme tous les hackers. Sauf, qu'il va avoir l'éthique vraiment au centre de son action et va essayer entre guillemets d'utiliser ses compétences pour le bien commun. Donc, quand il veut trouver une faille de sécurité par exemple dans une application mobile dans une entreprise. Quand il trouve des données, il va essayer de contacter l'entreprise en question, les personnes concernées pour que l'entreprise protège un petit peu mieux ses données, ses utilisateurs et son application globale. (03:45)

- **Certains outils utilisés par des malfaiteurs peuvent menacer notre sécurité. Informé des dangers qui existent, le gouvernement pourrait guetter notre empreinte numérique dans le but d'éloigner des dangers.**
  - Baptiste Robert : (…) donc ça vous le voyez c'est un câble standard d'iPhone, mais en réalité en fait à l'intérieur ici là vous allez voir un circuit imprimé qui permet de contacter en fait à distance le téléphone qui va être branché au câble. Je laisse ça par exemple dans un endroit public, voilà vous allez brancher pour recharger votre téléphone et en fait je vais prendre le contrôle juste parce que vous avez branché. (12:40)
  - Baptiste Robert : Le troisième, en fait, c'est un petit objet qu'on peut se balader. En gros ça va être une bande wifi. En fait, cela va être ma bande wifi, donc je vais pouvoir, si vous vous connectez là-dessus… Donc je vais l'appeler, par exemple, Clique-Guest et donc vous allez vous connecter dessus et je vais pouvoir voir tout le trafic qui passe. Mais même sans vous connecter en fait, juste si je l'allume, je vais savoir tous les wifi qui sont enregistrés sur vos téléphones. (13:28)

- **Nous ne pouvons guère nous responsabiliser de tout ce qu'il faut faire pour nous protéger. À part des outils malsains évoluent très vite, notre nature humaine est une faiblesse face aux attaques. Les organismes qui surveillent notre empreinte numérique peuvent nous épauler. Baptiste Robert offre plusieurs exemples qui affirment notre faiblesse (05:50). Même si le téléphone « ne va pas ouvrir le micro sans… autorisation ».**
  - « on est très très gentil, on lui donne beaucoup, beaucoup de données donc en fait, quand vous utilisez votre téléphone, quand vous utilisez TikTok par exemple, vous n'envoyez pas qu'une vidéo, vous envoyez plein de données autour. » (05:50)

Des pistes pour des réponses :

Non, je ne suis pas d'accord. La surveillance de notre empreinte numérique par les agences gouvernementales, bancaires et commerciales n'est pas justifiable.

(suite à la page 26)

Codes et pondération de chaque tâche :

Dans le document « Menace sur la cybersécurité » :

- **Nous tombons souvent victimes de la paranoïa en pensant que tout le monde cherche à nous voler. Bien qu'il y ait certains hackers qui font des choses illégales, « Tous les hackers ne sont pas des criminels sans foi ni loi, loin de là! (…) (§ 8) Certains d'entre eux développent des logiciels libres, d'autres garantissent la liberté de la presse ou cherchent les failles des logiciels que nous utilisons afin de les corriger. » (§ 8)**

- **Les organismes ont des « experts en sûreté et en sécurité » (§ 19) qui travaillent « au quotidien pour que notre navigation et nos échanges se déroulent avec une transmission fiable d'informations, autour de dispositifs capables de résister à une action malveillante. » (§ 19) De plus, « Pour que les numéros de cartes bancaires et nos conversations privées ne soient pas accessibles à n'importe qui sur le web, les informations sont donc cryptées : on parle de chiffrement des données. » (§ 19) Avec ces mesures déjà en place, nous n'avons pas besoin d'ouvrir notre empreinte numérique à des agences supplémentaires.**

- **Le texte nous assure de l'efficacité du chiffrement, ce qui enlève tout besoin d'une agence pour surveiller notre empreinte numérique.**
  - « Le chiffrement permet non seulement de protéger des données contre un vol ou une menace, mais aussi de prouver que les informations sont authentiques. Il garantit que le message provient de la bonne personne et n'a pas été transformé. » (§ 26)
  - « Les systèmes de cryptage des données sur le web sont de plus en plus répandus et de plus en plus complexes. » (§ 27)
  - Les clés symétriques et asymétriques sont utilisées ensemble pour créer un système plus sécuritaire. « Cette méthode utilise deux clés différentes pour le codage et le décodage d'un message. Ce système plus complexe est aussi plus sécurisé. » (§ 30)

- **Comme utilisateurs de la technologie, nous nous éduquons tous les jours sur des stratégies à implanter pour détourner ceux qui souhaitent nous voler de notre identité. Plusieurs stratégies sont clairement affichées à la page 50 :**
  - « préférer des mots de passe intégrant des caractères spéciaux, des majuscules et des chiffres… » (§ 43)
  - fuyez des sites avec ce qui semble « douteux, avec des fautes d'orthographe ou un logo étrange. » (§ 44)
  - « soyez prudents sur des postes informatiques partagés ou si vous utilisez des clés USB : c'est par ces supports que circulent aisément des logiciels espions… » (§ 47)
  - « un bon antivirus et un pare-feu, des sauvegardes régulières sur un support déconnecté » (§ 47)

Dans le document audiovisuel :

- **Même avec toutes les ressources disponibles, le gouvernement ne peut guère se protéger. La question se pose : comment peut-il alors nous protéger? Nous devons tout simplement nous fier à notre capacité de surveiller l'état de notre empreinte numérique.**
  - En se référant à Baptiste Robert, Mouloud dit : (…) Vous avez repéré des failles de sécurité sur des sites et des applications qui appartenaient aux gouvernements français, indiens et américains. (04:21). Robert Baptiste affirme : J'avais accès à tous les groupes de messagerie, j'avais accès aux contacts, j'avais accès voilà. (05:15)
  - Baptiste Robert divulgue : J'ai beaucoup travaillé sur le cyberespace indien, donc j'ai trouvé une faille dans l'application du Premier ministre indien, par exemple, et alors ce qui était assez rigolo en fait, c'est que j'ai publié quelque chose sur Twitter relatif à ça et 30 secondes après, j'ai le bureau du Premier ministre qui m'a contacté. (11:57)

- **Le hacker éthique, Baptiste Robert, nous outille des «trucs» à suivre pour nous protéger. Nous n'avons pas besoin d'agences pour surveiller nos empreintes numériques. Nous sommes déjà équipés pour y réussir.**
  - Refuser de mettre l'adresse courriel pour nous brancher au wifi d'un aéroport.
    - Baptiste Robert :… vous êtes à l'aéroport, vous vous connectez au wifi de l'aéroport, on vous demande une adresse email. Et en fait, pour accéder au wifi, vous n'avez pas besoin de l'e-mail fondamentalement et si vous mettez n'importe quoi, ça va quand même marcher. (09:34)
    - Yasine confirme : Vous mettez mail@mail ça marche très bien. (09:59)
  - Créer et maintenir une fausse identité dans certaines situations.
    - Baptiste Robert : C'est un conseil que je donne souvent, c'est qu'il faut mentir et mentir régulièrement de manière consistante. C'est-à-dire qu'il faut se créer une identité : aujourd'hui, je m'appelle Baptiste Robert sur Internet. Demain je m'appelle John Doe, j'aurais un autre âge, après-demain je m'appellerais Jane Doe, je serais une femme et j'aurais encore un autre âge. C'est de mentir de manière constante, régulièrement. (10:15)
  - Utiliser deux adresses.
    - Mouloud : J'ai deux adresses pour ces choses-là moi… (10:35)

- **Le hacker éthique, Baptiste Robert, nous informe des «petits jouets» des hackers. En nous informant de la technologie, nous pouvons gérer l'état de notre empreinte numérique.**
  - Baptiste Robert : On va avoir une première clé USB qui est une clé USB assez simple et en fait qui permet d'automatiser en gros le hacking. Typiquement, cette clé USB, elle a été utilisée dans une situation précise. (10:44)
    Cela a été utilisée pour télécharger des informations d'un ordi d'une guichetière d'une banque.

(suite à la page 28)

Codes et pondération de chaque tâche :

- Baptiste Robert : (…) donc ça vous le voyez c'est un câble standard d'iPhone, mais en réalité en fait à l'intérieur ici là vous allez voir un circuit imprimé qui permet de contacter en fait à distance le téléphone qui va être branché au câble. Je laisse ça par exemple dans un endroit public, voilà vous allez brancher pour recharger votre téléphone et en fait je vais prendre le contrôle juste parce que vous avez branché. (12:40)
- Baptiste Robert : Le troisième, en fait, c'est un petit objet qu'on peut se balader. En gros ça va être une bande wifi. En fait, cela va être ma bande wifi, donc je vais pouvoir, si vous vous connectez là-dessus… Donc je vais l'appeler, par exemple, Clique-Guest et donc vous allez vous connecter dessus et je vais pouvoir voir tout le trafic qui passe. Mais même sans vous connecter en fait, juste si je l'allume, je vais savoir tous les wifi qui sont enregistrés sur vos téléphones. (13:28)

Toute autre réponse dûment appuyée sur des éléments de textes.

Tableau pour transposer la note sur 50 points

Résultat de l'élève sur 20	Résultat de l'élève sur 50
20	50,0
19	47,5
18	45,0
17	42,5
16	40,0
15	37,5
14	35,0
13	32,5
12	30,0
11	27,5
10	25,0
9	22,5
8	20,0
7	17,5
6	15,0
5	12,5
4	10,0
3	7,5
2	5,0
1	2,5
0	0,0