Le télétravail: quels impacts juridiques?

Juin 2020

Vanessa Henri

avocate - technologies émergentes, gouvernance des données et cybersécurité

FASKEN

Une nouvelle nécessité

- **Zoom:** Actions + 50%; Nombre d’utilisateurs actifs par jour: +378%; Usage par jour: +300%
- **Teams:** +775% d’utilisation (utilisateurs des appels et rencontre en Italie), 44M d’utilisateurs actifs à chaque jour.
- **WebEx**: 50M de rencontres juste dans les trois premières semaines de mars.

Une réalité inquiétante

MONTREAL | News

Police officers' personal information may be at risk after ransomware data hack

The Canadian Press Staff
Contact

Published Wednesday, October 28, 2020 4:55PM EDT

Attaque informatique: la STM a été infectée par hasard via un courriel

PARTAGEZ SUR FACEBOOK PARTAGEZ SUR TWITTER AUTRES

A Patient Dies After a Ransomware Attack Hits a Hospital

The outage resulted in a significant delay in treatment. German authorities are investigating the perpetrators on suspicion of negligent manslaughter.

EDITORS' PICK | 21,127 views | Jul 4, 2020, 07:03am EDT

Stuxnet 2? Iran Hints Nuclear Site Explosion Could Be A Cyberattack

Kate O'Flaherty Senior Contributor
Cybersecurity
I'm a cybersecurity journalist.

Russians Who Pose Election Threat Have Hacked Nuclear Plants and Power Grid

The hacking group, Energetic Bear, is among Russia's stealthiest. It appears to be casting a wide net to find useful targets ahead of the election, experts said.

ACCUEIL | INFO | SOCIÉTÉ | SANTÉ |
COVID-19 : TOUT SUR LA PANDÉMIE

Une attaque informatique cible des hôpitaux canadiens et américains

de la Santé du Québec fait partie des
cette campagne agressive de demande de

Les obligations contractuelles

Les contrats peuvent contenir des clauses relatives à la sécurité de l'information qui ne sont pas nécessairement suspendues par raison de COVID-19 ou du télétravail..

Peut-on invoquer la force majeure?

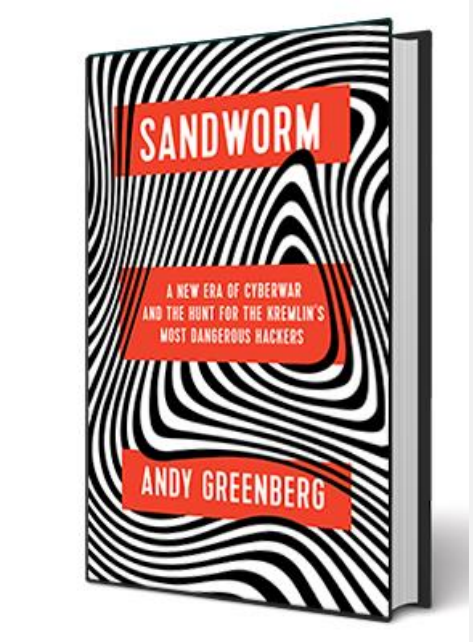
1470. Toute personne peut se dégager de sa responsabilité pour le prejudice causé à autrui si elle prouve que le prejudice résulte d'une force majeure, à moins qu'elle ne se soit engage à la réparer.

La force majeure est un évènement imprévisible et irresistible, y est assimilée la cause étrangère qui présente ces mêmes caractères.

Les obligations réglementaires

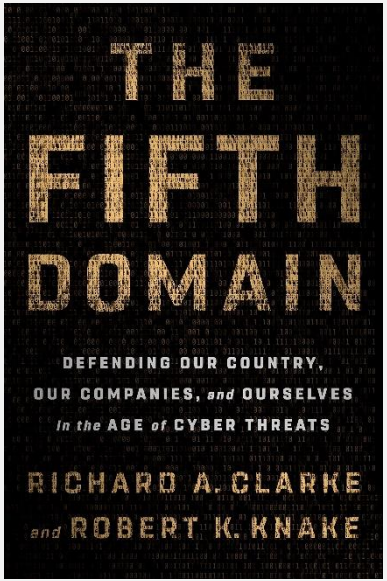
- Lois sur les renseignements personnels (national, fédéral, etc.)
- Directrice des autorités sur la sécurité lors du télétravail (ex: CNIL)
- Certains decrets accordant des exemptions pour assurer une transformation numérique accélérée durant COVID-19 (ex: HIPAA)
- Obligations additionnelles (e.g. logiciels médicaux)
- Attention aux compagnies publiques…

Il n’y a pas juste les brèches de renseignements…



- Cyber-espionage industriel et politique
  - Qui se rappelle Moonlight Maze?
- Attaques à la disponibilité souvent sous-estimées, comme les “DDoS”
- Attaques cyber-physiques
- Attaques aux infrastructures critiques

Quelle autorité sur l'infrastructure domestique des employés?

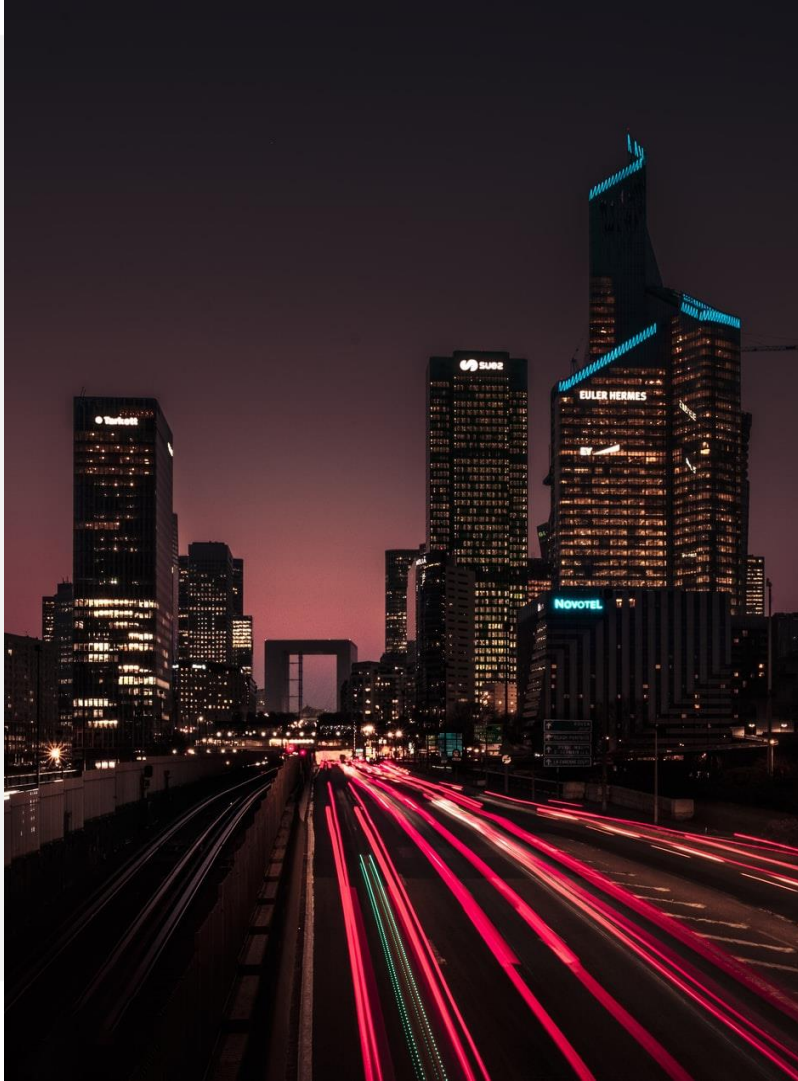


- "The corporate frontline" – *The Fifth Domain,* Richard A. Clarke & Robert K.Knake.

"Each major U.S. bank spends more than half a billion dollars on cyber defense every year. Arrayed against the cyber criminal gang's hacker-tool-development team, there are more than several hundred bank and contractor employees defending the network […] The defenders will usually not attack, because they can't. If they are corporations, by law they are not allowed to. […] Ultimately, a bank isn't spending half a billion dollars to keep out one attacker. It is spending half a billion dollars to keep out one attacker. It's spending half a billion dollars to protect many trillions of assets from more than two hundred advanced persistent threat group. By one estimate, there are seventy-seven Chinese APT groups alone."

Rôles des entreprises

- Les entreprises sont la première ligne de défense, car elles sont propriétaires des infrastructures. Les gouvernements ne peuvent donc pas assister directement, comme dans d’autres “guerres”.
- Au même titre, les entreprises ne sont pas propriétaires des réseaux et équipement TI des employés.
- Il faut donc trouver d’autres moyens de sécuriser le nouvel espace de travail.



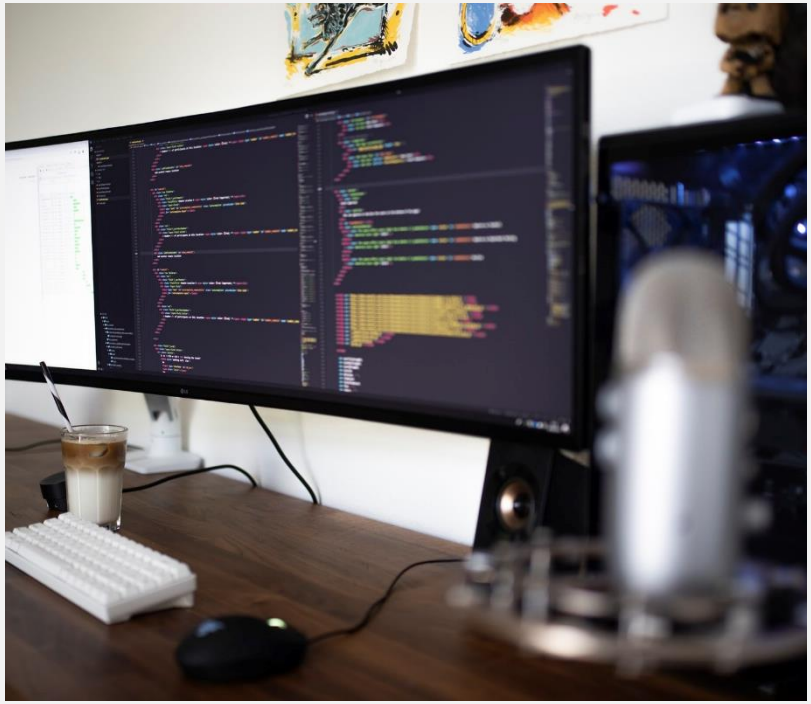
Sécuriser ce qui ne nous appartient pas…

- Est-ce que la sécurité des réseaux a perdue son importance avec le DevSecOps et les connexions virtuelles par VPN?
  - Cyber-guerre de l'Estonie: Prise de possession de "routers" Internet pour paralyser l'utilisation de l'Internet et des services comes les ATMs.
  - Menaces reliées aux IoT et objets connectés, incluant les routers: possibilité de DDoS.
- En tant que pays, nous sommes aussi sécuritaire que notre plus faible maillon, et si notre plus faible maillon sont nos employés… nous risquons de perdre notre infrastructure de travail virtuel. C'est donc plus qu'une question de protection des *actifs informationnels*, il faut continuer de protéger les infrastructures!

Tendez la maison aux employés

- Avez-vous expliquez aux employés comment vérifier s’ils utilisent un chiffrement WPA2 ou WPA3, ainsi qu’un mot de passe suffisant?
- Avez-vous expliquez aux employés comment configure un router, ou bien comment créer des réseaux invités?
- Avez-vous considérez envoyer des routers pour vos employés qui ont des accès privilégiés, afin que vous puissez les gérer vous même?

La conformité interne

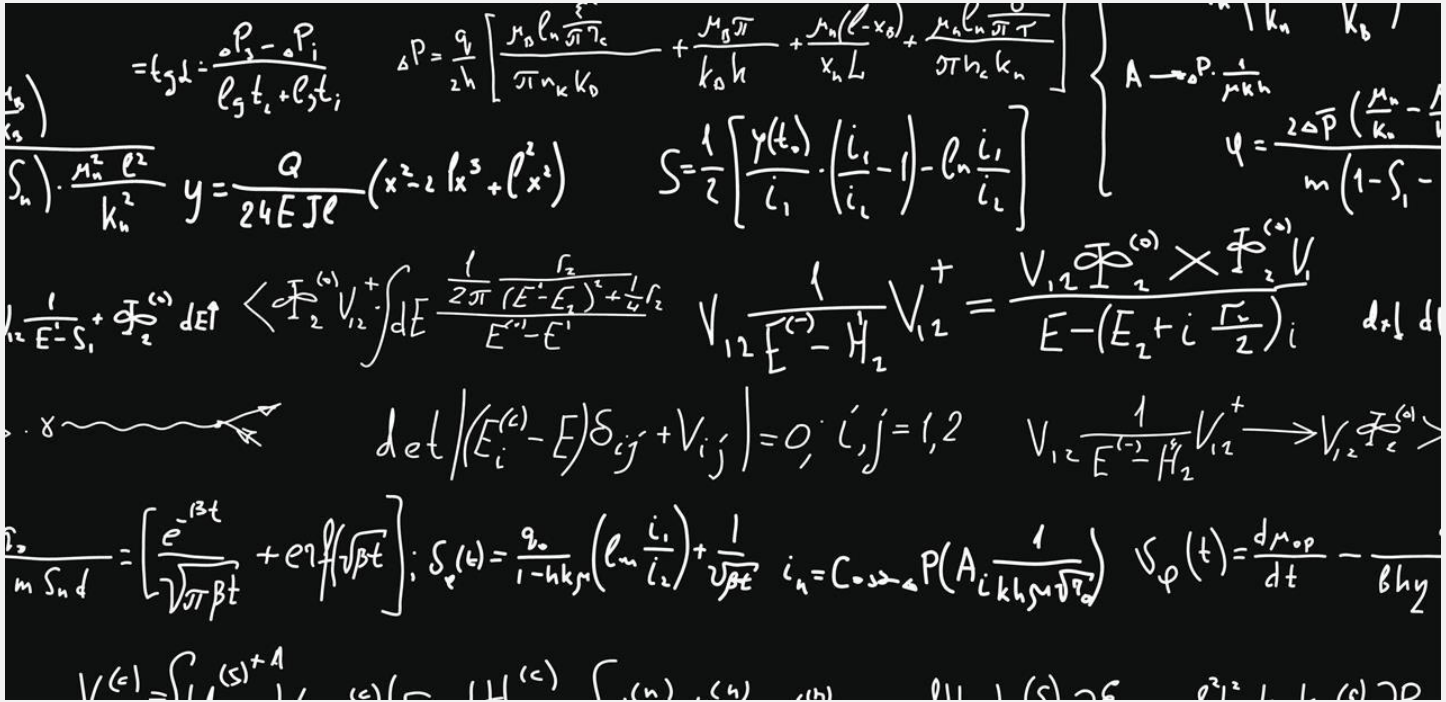


- Les politiques relatives au télé-travail:
  - Ont-elles été revues et ajustées, ou bien avez-vous implémentées dans exceptions?
  - Comment gérer les deviations des politiques en cas de force majeure?
  - Rappelez-vous… Les employés ont l'obligation juridique de suivre les normes internes.
- Pourquoi ne pas préparer des lignes directrices sur des mesures précises que les employés peuvent prendre pour sécuriser leurs infrastructures personnelles?

Évaluez les impacts

- Comment allez-vous procéder à un e-discovery suivant une brèche si l'employé est localise chez lui?
- Devez-vous avoir un mandat pour venir saisir l'ordinateur? Pour pouvoir inspecter le lieu de travail dans la maison?
- Pouvez-vous enquêter sur les technologies et hardware qui ne vous appartiennent pas?
- Le télétravail oui… mais si le télétravail se passe à l'étranger, quels impacts?

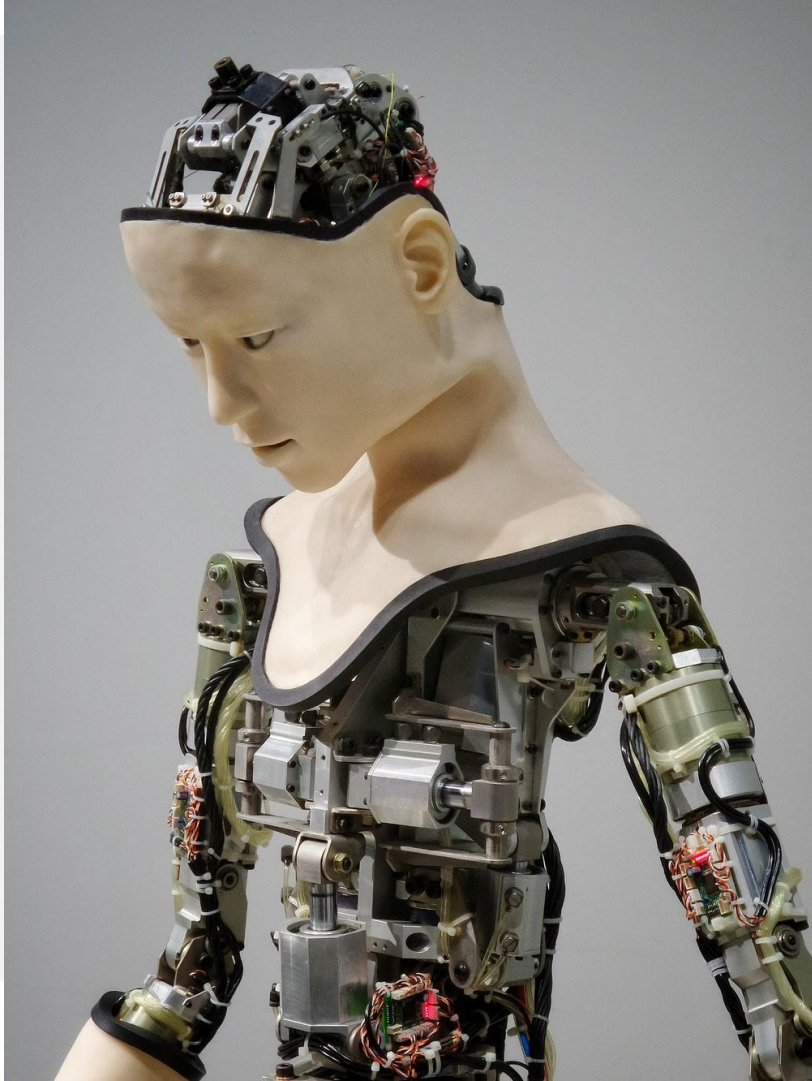
Algorithmes prédictifs



FASKEN

Technologies émergentes

- Attention au traitement automatisé des données avec impacts juridiques sur les individus
- Avoir des mécanismes de revue en place
- Attention à la qualité des données utilisées, demandez-vous s’il s’agit des bonnes données pour le bon algorithme.
- Avez-vous considérez les risques particuliers comme le “data poisoning?”



Attention aux produits de sécurité…

- Ils peuvent aussi contenir des vulnérabilités. Le nombre de vulnérabilités moyen pour les produits de sécurité oscille entre 18% à 44%*.
- Pour accélérer la digitalisation, plutôt que d’éviter de faire des verifications, considerer des produits d’analyse en temps réel pendant le travail DevOps (e.g. GreenLight de Veracode) et l’utilisation de produits AI/ML… mais attention! Ils peuvent être biaisé.

* The Fifth Domain, p. 79.

Négocier des contrats en période de transformation numérique accélérée

FASKEN

Liste de vérification

- Renseignements personnels
- Brèche de sécurité
- Propriété intellectuelle
- Moyen de resolution des disputes
- Limitations de responsabilité
- Limitations à l’usage
- Modifications unilatérales
- Droit de la consummation
- Remède en cas de défaillance des services
- Support technique

L’Internet des choses et les maisons intelligentes, quels impacts?

- Éviter les assistants intelligents, sauf si approuvé par l’entreprise
- Éviter l’utilisation de IoT dans l’espace de bureau
- Attention aux maisons intelligentes, qui ne sont pas toujours si intelligente et peuvent introduire plusieurs vulnérabilités dans l’environnement de travail
- Attention aux imprimantes maisons et aux scanners par applicable mobile sur les téléphones: ce sont des raccourcis dangereux que les employés prennent si vous ne donnez pas de bonne alternative!
- Pensez aux outils comme les signatures numériques.

Surveillance des employés

- Au Québec, les renseignements personnels des employés sont protégés par la loi. Vous devez avoir un consentement implicite ou explicite, ou bien une exception législative.
- Il s'agit souvent de mesures très intrusives, dans un environnement qui n'est pas le vôtre, soit dans une demeure privée.
- Conduisez une analyse des facteurs reliés à la vie privée, et déterminer comment vous allez mitiger les impacts, combien de temps vous allez gardez les données recueillies, etc.
- *Est-ce vraiment nécessaire?* Nous n'avons pas d'exemples de réussite flagrante! La confiance a bien meilleur gout… et la gestion des accès!

Attention à l’aspect humain…

TRENDING

Journalist Jeffrey Toobin apologizes after exposing himself on Zoom call

By Josh K. Elliott · Global News
Posted October 20, 2020 9:09 am · Updated October 20, 2020 3:46 pm

- Le déplacement du bureau à la maison peut mener à des situations embarassantes. Doit-on les traiter comme des brèches de sécurité, ou bien doit-on avoir aussi un aspect humain pour supporter l’individu, qui peut être embarassé?

Vanessa Henri
Lawyer
+1 514 397 7497
vhenri@fasken.com

FASKEN

FASKEN