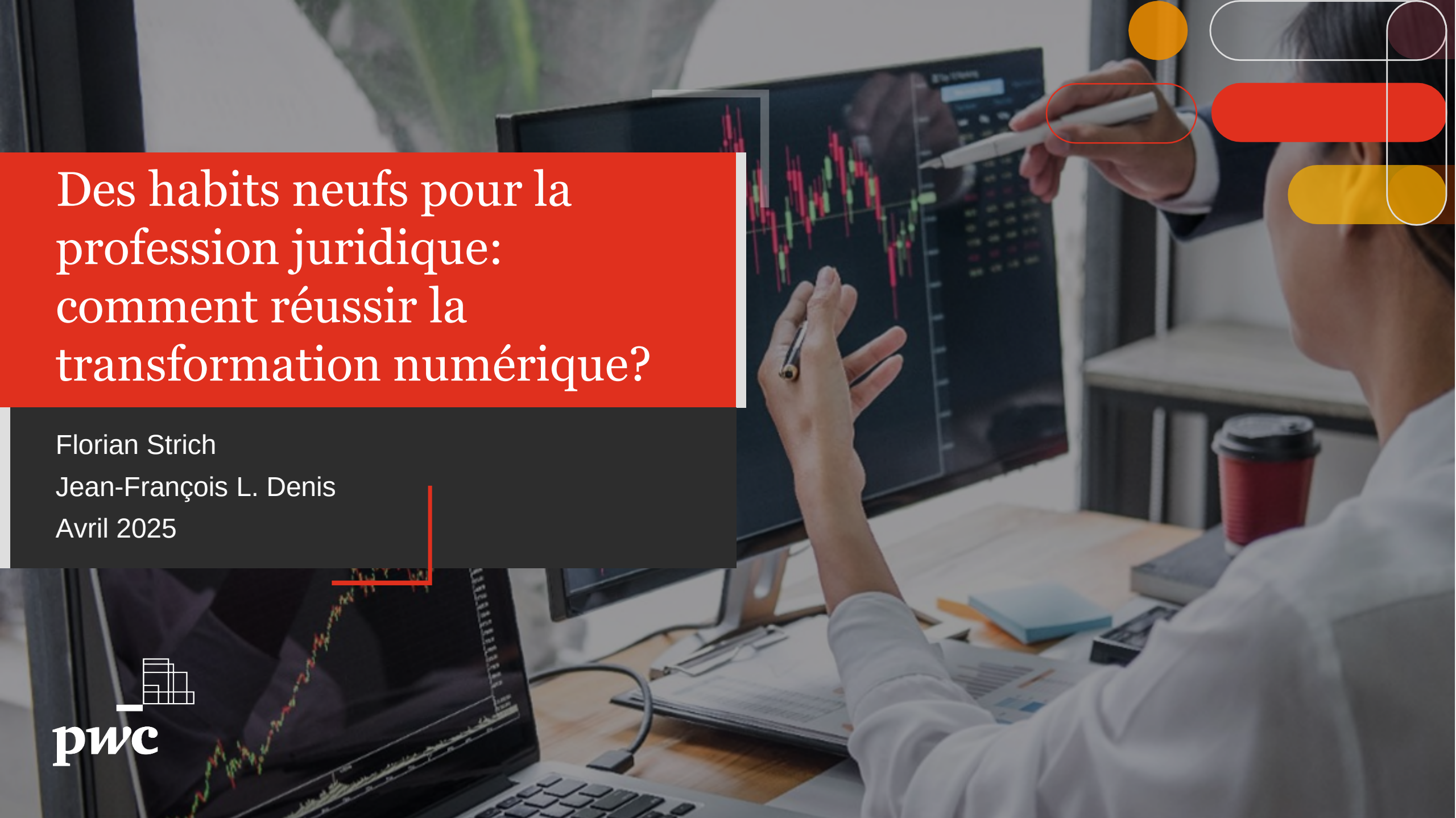
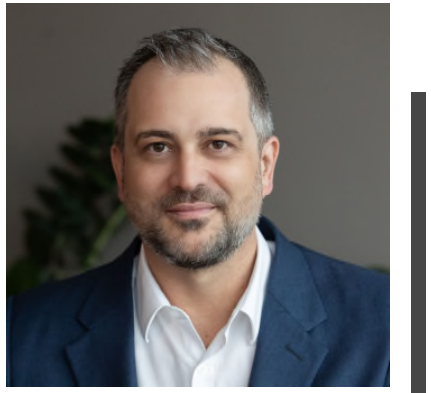


Des habits neufs pour la profession juridique: comment réussir la transformation numérique?

Florian Strich
Jean-François L. Denis
Avril 2025

Vos conférenciers



Jean-François L. Denis

Jean-Francois.L.Denis@pwc.com

Leader, Est du Canada, Solutions d’affaires juridiques

Florian Strich

Florian.Strich@pwc.com

Premier directeur, Protection de la vie privée

Agenda

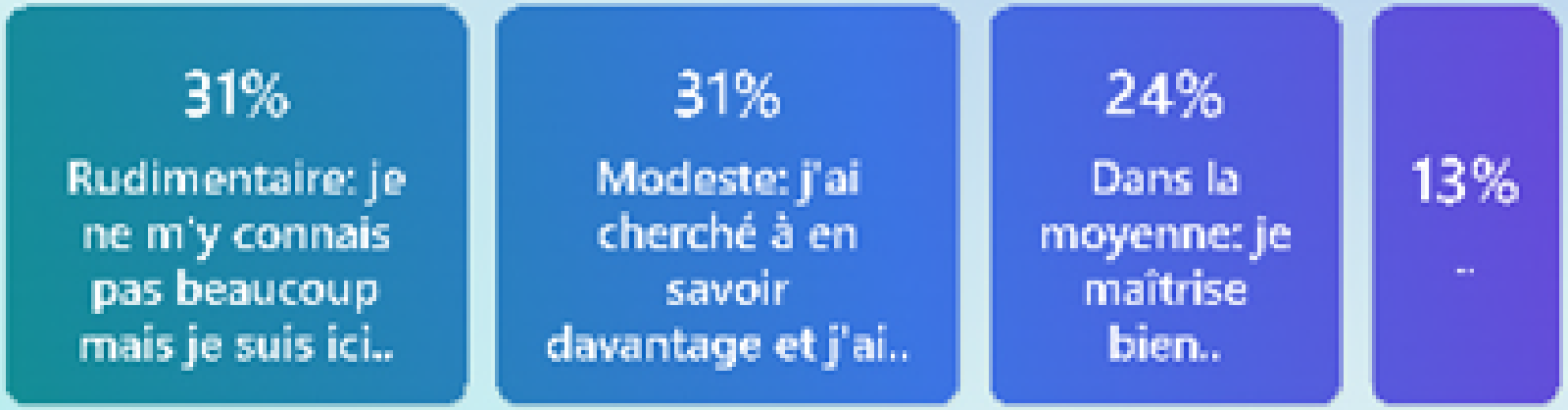
Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/xMDkEnwjAB

Copier le lien

29 réponses envoyées

Comment décrivez-vous votre niveau de connaissances en ce qui a trait à la transformation numérique de la pratique du...



Carte proportionnelle | Barre

1 sur 1

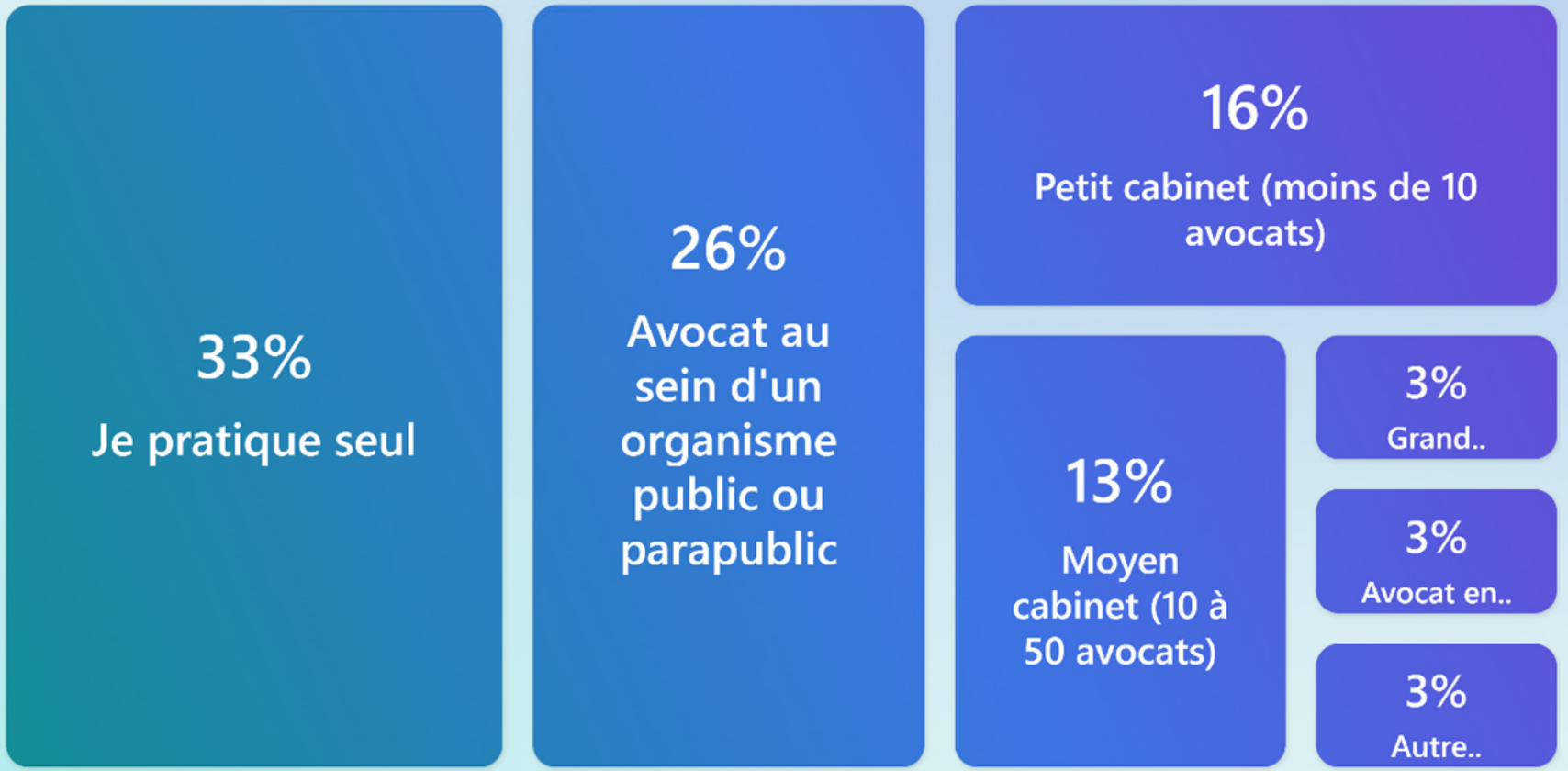
Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/rQpEVtu2M0

Copier le lien

30 réponses envoyées

Qu'est-ce qui décrit le mieux votre pratique à l'heure actuelle?



Carte proportionnelle | Barre

1 sur 1

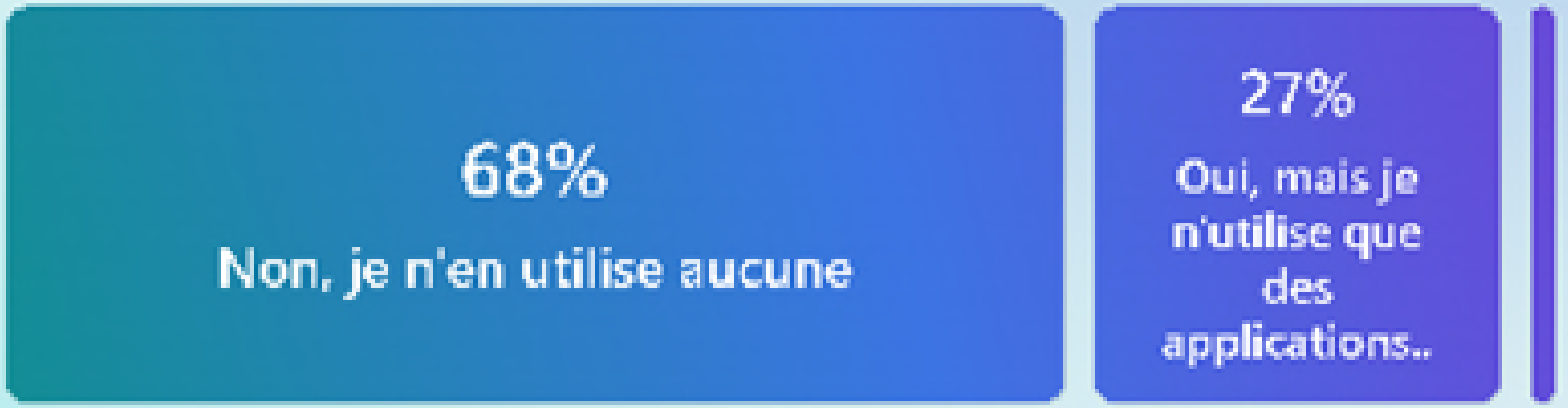
Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/bdZSbVhapu

Copier le lien

29 réponses envoyées

Utilisez-vous une ou des applications d'intelligence artificielle?



Carte proportionnelle | Barre

1 sur 1

Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/fD4EPDfktw

Copier le lien

28 réponses envoyées

De façon générale, faites-vous confiance aux applications d'intelligence artificielle générative?

Carte proportionnelle | Barre

1 sur 1

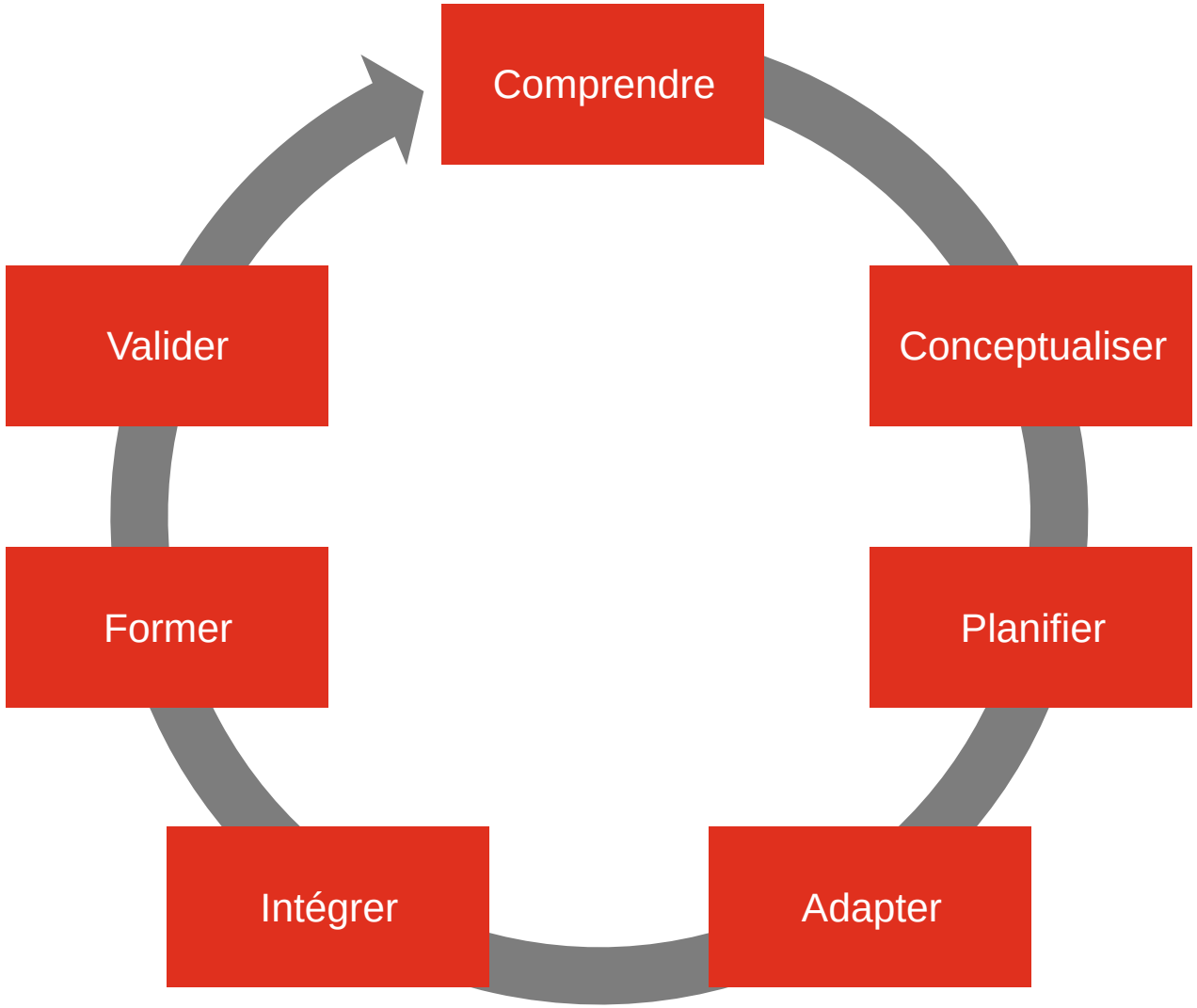
Partie 1

Introduction à la transformation numérique pour les praticiens du droit

Qu’est-ce que la transformation numérique

Québec Office québécois de la langue française

Démarche visant le **changement** en profondeur d'une organisation par l'intégration de **technologies** numériques à **l'ensemble de ses processus** administratifs, de ses communications et de ses activités, par la refonte de son **modèle d'entreprise** et par l'adaptation de sa **culture** organisationnelle aux nouvelles réalités du numérique.



Pourquoi prendre le virage numérique?

Amélioration de l’efficacité et de la productivité	• Cible: tâches répétitives et administratives, généralement à faible valeur ajoutée • But: libérer du temps pour les avocats, emphase sur les services à haute valeur ajoutée
Réduction des coûts opérationnels	• Dématérialisation • Collaboration
Amélioration de la qualité et de la précision	• Identification des erreurs ou des incohérences • Analyse prédictive basée sur des données • Prise de décision optimisée
Meilleure gestion des risques et conformité	• Outils de suivi et de conformité plus efficaces • Potentiel d’automatisation • Atténuation en amont des risques potentiels
Amélioration de l’expérience client	• Services plus rapides, plus personnalisés • Services accessibles en ligne • Mise à jour en temps réel

Mettre les chances de votre côté: comment réussir la transformation numérique

75%

Des transformations numériques se terminent par un échec.

70%

De ces échecs sont dus à un faible engagement des employés et à l'absence de changement des comportements.

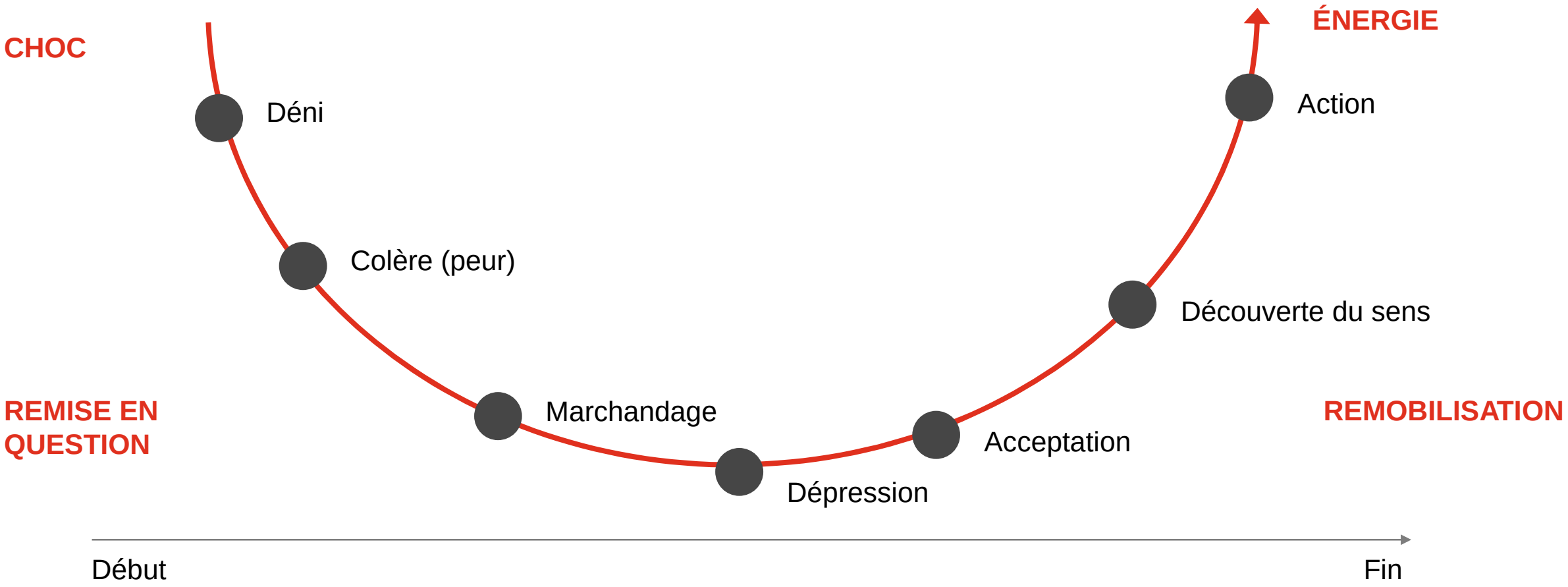
3 règles d'or

- Problème > Solution
- Pas une tâche informatique!
- Placer l'humain au cœur du projet

5 reasons your people will make or break your digital transformation

Mettre les chances de votre côté: comment réussir la transformation numérique (suite)

Les étapes prévisibles de tout processus de changement



5 Kubler-Ross Change Curve

Comment placer l’humain au centre de l’exercice?

1 Le changement, c’est difficile

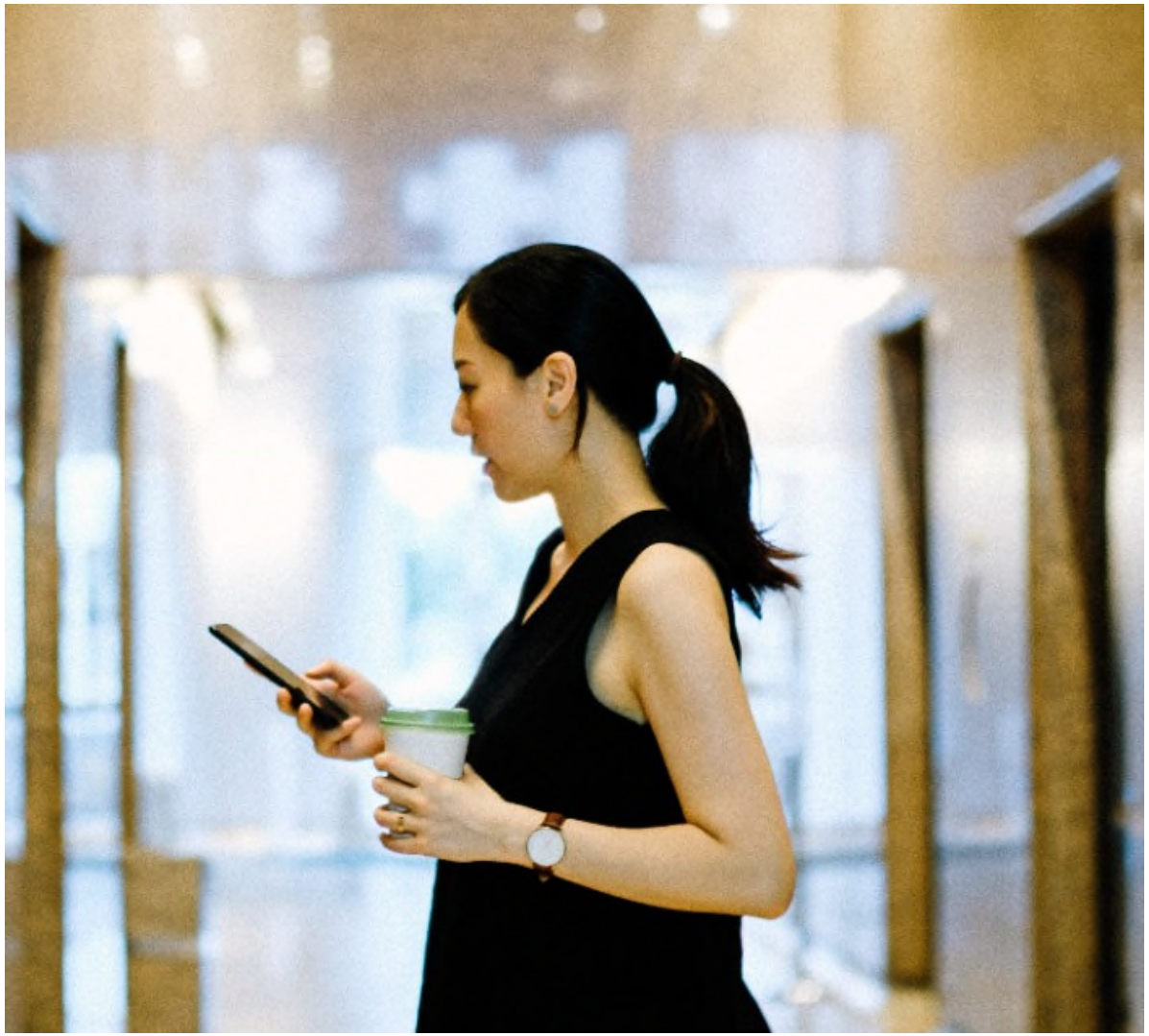
- Les gens sont différents
- On s’attend à ce que la technologie soit facile à utiliser
- L’importance des leaders
- La fatigue va gagner vos équipes
- Le changement prend tu temps

5 Reasons your people will make or break your digital transformation

Comment réussir sa transformation numérique?

1 3 clés pour le succès

- Travailler avec des experts
- Le tiers du budget = adoption
- Écouter vos équipes



5 Reasons your people will make or break your digital transformation

Partie 2

Technologies clés et leur impact sur la profession juridique

Aperçu des technologies

Gestion des Documents et des Dossiers

- **Systèmes de Gestion de Documents (DMS)** : iManage, NetDocuments, Worldox
- **Systèmes de Gestion de Cas (CMS)** : Clio, MyCase, PracticePanther, Legal Suite, Mitratech Team Connect, Onit
- **Outils de Collaboration et de Partage de Fichiers** : SharePoint, Google Drive, Dropbox, Nota Bene

Aperçu des technologies (suite)

Recherche juridique

- **Bases de Données Juridiques** : LexisNexis, Westlaw, Bloomberg Law, SOQUIJ, Canlii.org
- **Outils de Recherche Assistée par IA** : ROSS Intelligence, Casetext, Judicata

Aperçu des technologies (suite)

Automatisation des documents

- **Génération Automatique de Documents** : HotDocs, Contract Express, DocuSign
- **Outils de Révision de Contrats** : Kira Systems, Luminance, LawGeex

Aperçu des technologies (suite)

Gestion de la relation client

- **Systèmes CRM** : Salesforce, HubSpot, Lexicata

Aperçu des technologies (suite)

Facturation et comptabilité

- **Logiciels de Facturation** : TimeSolv, Bill4Time, Zola Suite
- **Logiciels de Comptabilité** : QuickBooks, Xero, FreshBooks

Aperçu des technologies (suite)

Sécurité et conformité

- **Outils de Sécurité des Données** : Symantec, McAfee, Norton
- **Solutions de Conformité** : ComplySci, Smarsh, Relativity, Compliance Insights (PwC)

Aperçu des technologies (suite)

Communication et collaboration

- **Outils de Communication** : Microsoft Teams, Slack, Zoom
- **Outils de Gestion de Projets** : Trello, Asana, Monday.com

Aperçu des technologies (suite)

Formation et développement professionnel

- **Plateformes de Formation en Ligne** : Coursera, Udemy, LinkedIn Learning
- **Outils de Simulation et de Réalité Virtuelle** : VR Law Room, Legal Tech VR

Aperçu des technologies (suite)

Outils de productivité

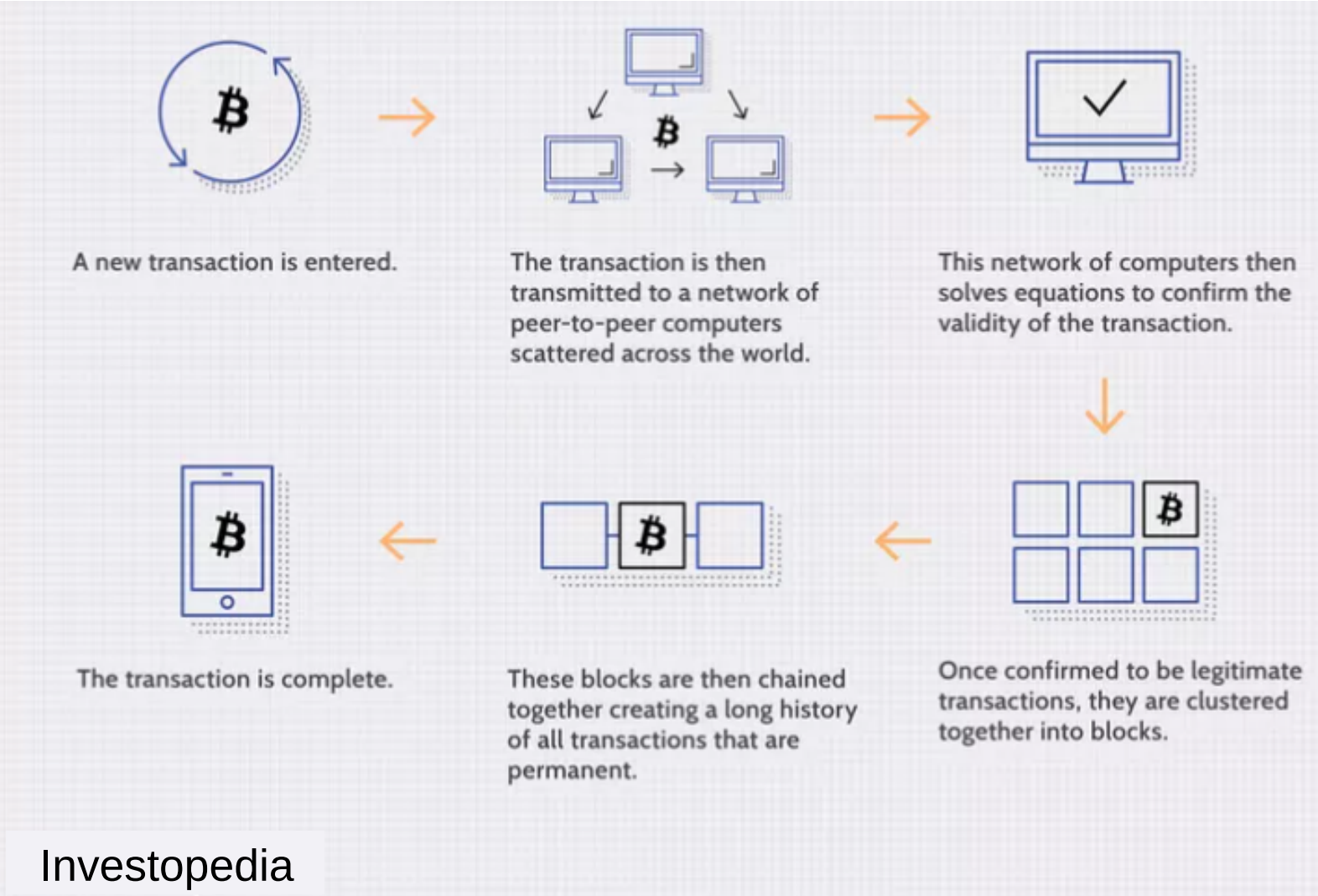
- **Suites Bureautiques** : Microsoft Office 365, Google Workspace
- **Outils de Gestion du Temps** : Toggl, RescueTime, Clockify

Aperçu des technologies (suite)

Technologies de Blockchain et Smart Contracts

- **Plateformes de Blockchain** : Ethereum, Hyperledger
- **Outils de Smart Contracts** : OpenLaw, Clause.io, Edilex

La stabilisation des cas d'usages de la blockchain



Investopedia

La blockchain est un registre numérique décentralisé qui stocke de manière sécurisée des enregistrements sur un réseau d'ordinateurs, de manière transparente, immuable et résistante à la falsification. Chaque "bloc" contient des données, et les blocs sont liés dans une "chaîne" chronologique. (Investopedia)

Cas d'usages juridiques

- Cryptomonnaies
- Contrats intelligents
- Cadastre

Aperçu des technologies

Outils de Résolution de Conflits en Ligne (ODR)

- **Plateformes de Médiation et d'Arbitrage en Ligne** : Modria, eJust, FairClaims

Aperçu des technologies (suite)

Technologies de Mobilité

- **Applications Mobiles pour Avocats** : Clio Mobile, MyCase Mobile, Fastcase

Aperçu des technologies (suite)

Outils de Marketing et de Développement de Pratique

- **Outils de Marketing Digital** : Hootsuite, Buffer, SEMrush
- **Outils de Gestion de Réputation** : Birdeye, Reputation.com, ReviewTrackers

Aperçu des technologies (suite)

Analyse de Données et Intelligence Artificielle

- **Outils d'Analyse Prédictive** : Premonition, Lex Machina, Ravel Law
- **Outils d'Analyse de Données** : Tableau, Power BI, Qlik

0 réponse envoyée

Craignez-vous que l'intelligence artificielle réduise votre volume d'affaires?

Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/RXVLek9uWW

Copier le lien

Oui

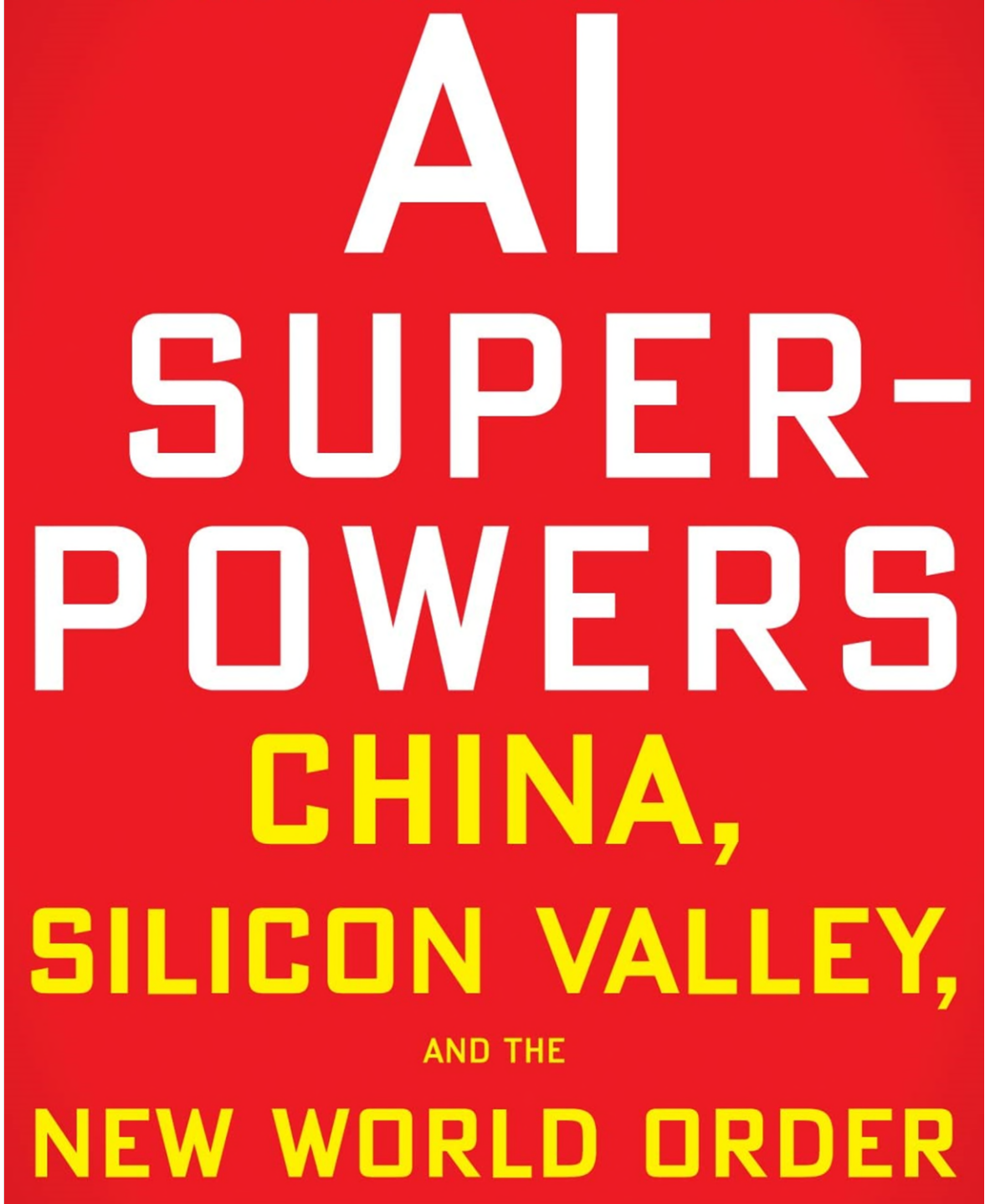
Non

Carte proportionnelle | Barre

1 sur 1

L'intelligence artificielle remplacera de nombreux emplois de cols blancs, y compris dans la profession juridique, à mesure que les algorithmes deviendront plus aptes à analyser des documents, prédire les résultats et automatiser la recherche juridique.

Kai Fu Lee
AI Superpowers



Qu'est-ce que l'IAG?

L'IA générative est une sous-catégorie de l'apprentissage profond qui consiste à entraîner un modèle pour générer de nouvelles données similaires aux données d'entraînement qui lui ont été fournies. Ce type d'IA peut être utilisé pour créer de l'art, de la musique, du texte et même des mondes virtuels entiers, entre autres applications.

Intelligence artificielle

L'IA est la théorie et le développement de systèmes intégrés dans un environnement, qui perçoivent, prennent des décisions et agissent pour atteindre un objectif spécifique.

Apprentissage automatique

Sous-domaine de l'IA axé sur la construction de systèmes qui améliorent automatiquement leurs performances au fil du temps et grâce à l'expérience.

Apprentissage profond

Technique d'apprentissage automatique basée sur des réseaux de neurones artificiels dans lequel plusieurs couches de traitement sont utilisées pour extraire des caractéristiques de plus en plus complexes à partir des données.

Intelligence artificielle générative

Algorithmes (tels que ChatGPT) qui utilisent une grande quantité de données et de grands modèles de langage (LLM) pour générer du nouveau contenu:

- Écrit: texte, code
- Visuel: images, vidéos
- Auditif: audio

Utilisés par des scientifiques

Maintenant accessible à tous

Les grandeurs de l'IAG au soutien de la pratique du droit

Automatisation de tâches répétitives

Analyse de données volumineuses

Prédiction de résultats juridiques

Amélioration des capacités de recherche juridique

Assistance à la rédaction de documents

L’atout principal: le coût!

Un phénomène particulier de l'IAG: les hallucinations

Les misères de l’IAG au soutien de la pratique du droit

Compréhension contextuelle

Confidentialité et sécurité

Jugement éthique et moral

Dépendance technologique et perte des réflexes

Compétences interpersonnelles

Quelques exemples de solutions déjà existantes

Predictice

Analyse prédictive qui aide les avocats à évaluer les chances de succès d'une affaire en se basant sur des données jurisprudentielles. Elle fournit des statistiques et des tendances pour éclairer les décisions juridiques.

NLPatent

Outil d'analyse de brevets alimenté par l'IA, utilisant le traitement du langage naturel pour confirmer ou infirmer l'existence de technologies similaires, identifier des tendances et optimiser les recherches de brevets.

PERSUIT

PERSUIT aide les entreprises à engager des conseillers juridiques externes. Sa plateforme aide les responsables juridiques à créer un impact commercial en rationalisant le processus d'engagement des conseillers externes.

LexisNexis

Améliore la recherche juridique et l'analyse de données, aidant les avocats à naviguer efficacement dans de vastes ensembles de données juridiques.

Quelques exemples de solutions déjà existantes

Harvey

Assistant juridique virtuel spécialement conçu pour le secteur juridique. Développée en partenariat avec OpenAI, cette plateforme utilise des modèles de langage avancés pour assister les avocats dans leurs tâches quotidiennes.

LeAh
ContractPodAi

Plateforme spécialisée dans la gestion du cycle de vie des contrats (CLM, Contract Lifecycle Management). Elle aide les services juridiques à automatiser et optimiser la création, la gestion et l'analyse des contrats.

laurel

Outil dédié à l'automatisation du suivi du temps pour les cabinets juridiques et comptables. Elle vise à optimiser la gestion du temps, augmenter la rentabilité et fournir des données précieuses pour améliorer l'efficacité opérationnelle et développer des *AFAs*.

Copilot

Microsoft 365 Copilot est un outil qui aide à effectuer des tâches de travail. Il offre des réponses sont en temps réel qui peuvent inclure du contenu internet et du contenu professionnel auquel les utilisateurs ont l'autorisation d'accéder.

Meilleures pratiques pour une utilisation responsable

Définir une stratégie

Définir ce que l'utilisation éthique des données signifie pour votre entreprise

- Quelles données peuvent être utilisées, lesquelles ne doivent pas l'être
- Inscrire l'utilisation dans les valeurs de votre entreprise et ses obligations réglementaires, juridiques, déontologiques

Objectif

Identifier des usages créant de la valeur tout en se conformant au cadre juridique applicable.

Meilleures pratiques pour une utilisation responsable (suite)

Identifier des mécanismes de contrôle

Analyser le cadre de gouvernance de votre entreprise (délégation d'autorité, gestion des risques, etc.)

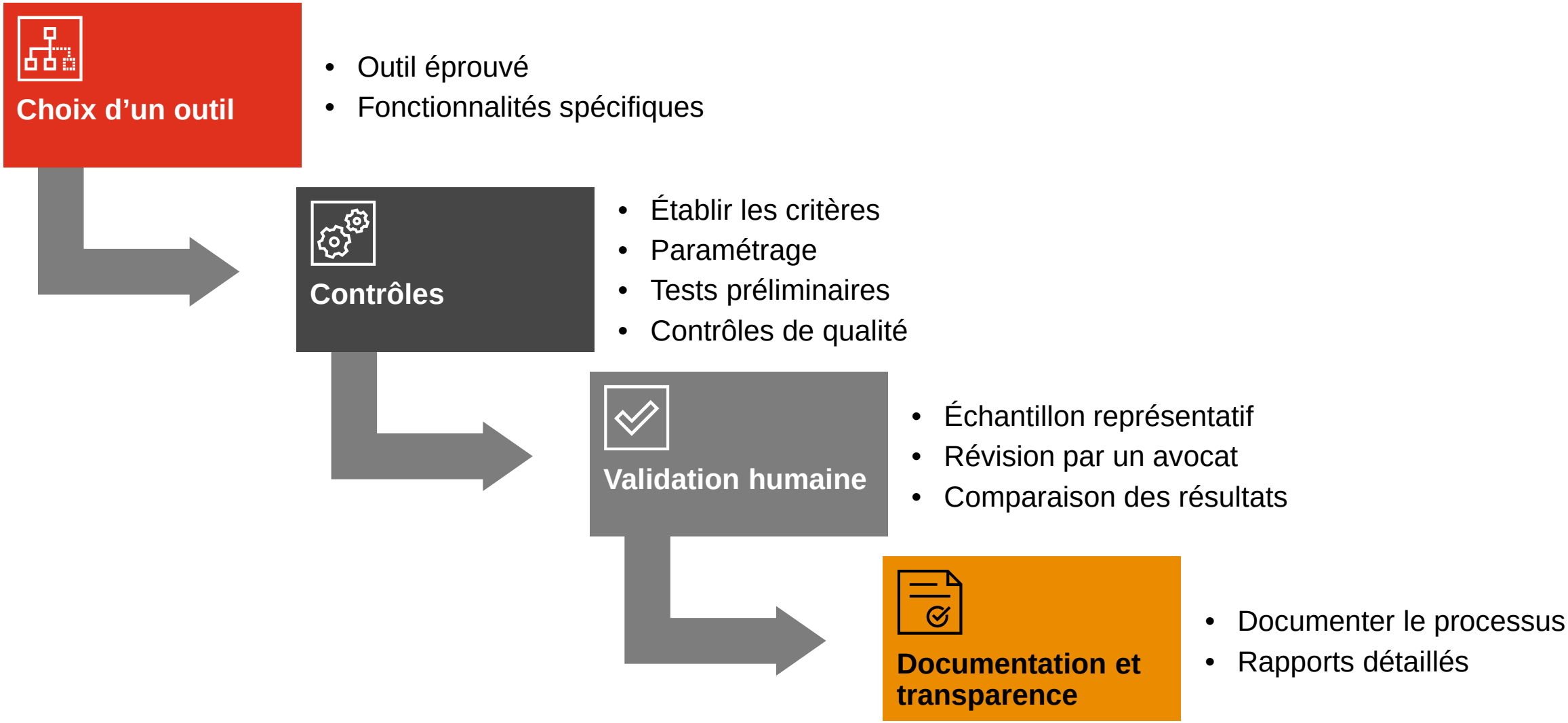
- Déterminer quelles politiques d'entreprise pourraient être touchées par l'utilisation de l'IAG (délégation d'autorité, gestion des risques, etc.)
- Valider le cadre juridique applicable et établir des contrôles en conséquence

Objectif

Définir et documenter des contrôles précis pour chaque cas d'usage

41

Pratique responsable: le choix d’un outil



Pratique responsable: validation requise

Calcul détaillé :

1. **Calcul initial de la taille de l'échantillon :** [n = \frac{(1.96)^2 \cdot 0.5 \cdot (1 - 0.5)}{(0.05)^2}] [n = \frac{3.8416 \cdot 0.25}{0.0025}] [n = \frac{0.9604}{0.0025}] [n = 384.16]

2. **Ajustement pour la taille de la population :** [n_{adj} = \frac{384.16}{1 + \frac{384.16 - 1}{3000}}] [n_{adj} = \frac{384.16}{1 + \frac{383.16}{3000}}] [n_{adj} = \frac{384.16}{1 + 0.12772}] [n_{adj} = \frac{384.16}{1.12772}] [n_{adj} \approx 340.68]

Conclusion :

Pour une population de 3000 contrats, avec un niveau de confiance de 95% et une marge d'erreur de 5%, un échantillon représentatif serait d'environ **341 contrats**.

Meilleures pratiques pour une utilisation responsable

Communiquer les pratiques responsables

Élaborer des lignes directrices claires encadrant l'utilisation de l'IAG

- Tenir compte de caractéristiques telles que l'explicabilité, la robustesse, l'impartialité, l'équité, l'originalité, la sécurité et la confidentialité

Objectif

Offrir un programme de formation continue à tous vos employés et se préoccuper de l'aspect validation

Meilleures pratiques pour une utilisation responsable (suite)

Développer des cas d'utilisation

Définir le contexte se prêtant à l'utilisation de l'IAG

- Toujours partir d'un problème à régler
- Remettre en question les pratiques en cours de route

Objectif

Alignement sur les cas d'utilisation et maintien des connaissances en temps réel

Partie 3

Intégration des outils numériques dans la pratique

Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/gQgEbvmNkj

Copier le lien

1 réponse envoyée

Au cours des 3 dernières années, avez-vous intégré de nouvelles technologies à votre pratique?

Carte proportionnelle | Barre

1 sur 2

L’intégration des technologies à la pratique: la clé du succès

Évaluation des Besoins et des Objectifs

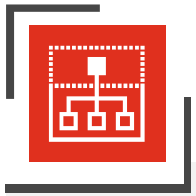
Sensibilisation aux Avantages

Formation et sensibilisation

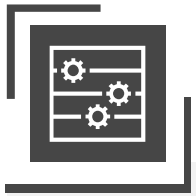
Sécurité et conformité

Intégration avec les Systèmes Existants

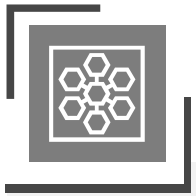
L’intégration des technologies à la pratique: la clé du succès (suite)



Gestion du changement



Suivi et évaluation



Support technique

Culture de l’innovation

Collaboration et communication

Partie 4

Aspects déontologiques, cybersécurité et protection des renseignements personnels

Aspects déontologiques

Compétence

Code de déontologie des avocats

- Article 20 (intégrité, compétence, loyauté, confidentialité, désintéressement, prudence)
- Article 21 (tenir à jour ses connaissances et habiletés)
- Article 22 (services de qualité)

Discrimination

Code de déontologie des avocats

- Article 4.1 (s'abstenir de toute discrimination)

Charte des droits et libertés de la personne

- Article 10 (motifs de discrimination)

Aspects déontologiques (suite)

Secret professionnel

Charte des droits et libertés de la personne

- Article 9 (droit au secret professionnel)

Code des professions

- Article 60.4 (droit au secret professionnel)

Loi sur le Barreau

- Article 131 (secret absolu des confidences)

Code de déontologie des avocats

- Article 20 (obligation d'intégrité, de compétence, de loyauté, de confidentialité, de désintéressement, de diligence et de prudence)
- Articles 60 et ss. (confidentialité)

Lois sur la protection des renseignements personnels dans le secteur privé et public (Loi 25)

- Article 10 (privé) et 63.1 (public) (assurer la protection des renseignements personnels)

Aspects déontologiques (suite)

Conservation

Règlement sur la comptabilité et les norms d'exercice professionnel des avocats

- Documenter les instructions
- Conservation: 7 ans suivant la fermeture

Supervision

Code de déontologie des avocats

- Article 5 (respect de la loi)
- Article 35 (ne pas multiplier inutilement les actes professionnels)
- Article 35 (responsabilité et supervision du mandat)

Confiance

Code de déontologie des avocats

- Article 23 (meilleur intérêt du client)
- Article 26 (communication)
- Article 28 (étendue du mandat, consentement)
- Article 37 (franchise, honnêteté)
- Article 38 (explications requises)

Aspects déontologiques (suite)

Honoraires

Code de déontologie des avocats

- Article 99 (modalités financières, accord, déviations)
- Article 101 (honoraires raisonnables)
- Article 102 (justification des honoraires)

Tribunaux

Code de déontologie des avocats

- Article 111 (soutien de l'autorité)
- Article 116 (ne pas induire en erreur)
- Article 132 (collaboration avec avocats, attitude déloyale)

1

Cybersécurité

Quelles sont les menaces qui pèsent sur les avocats ?

Les informations présentées ici sont pour la plupart issues du Guide des TI gestion et sécurité des technologies de l'information pour l'avocat et son équipe (lien) édité par le barreau du Québec en janvier 2016

Les menaces exploitent des	Vulnérabilités de l'entreprise dans:
Incident de confidentialité malveillant ou non, interne ou non	• La sécurité des télécommunications (technologies réseau, serveurs, réseaux d'accès, etc.) • La sécurité des infrastructures matérielles (salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail personnels, etc.) • La sensibilisation des utilisateurs (formation des employés, processus internes conformes et politique en matière de sécurité, etc.)
Rançongiciel (Ransomware)	
Hameçonage (Phishing)	
Logiciel malveillant (Malware)	
Attaque de l'homme du milieu (Man in the middle)	
Ingénierie sociale	
Intrusion physique	
Catastrophe naturelle	

Il s'agit fondamentalement de protéger le secret professionnel dans un contexte de technologies de l'information

Concepts clés

Confidentialité, Intégrité et Disponibilité, les 3 commandements de la cybersécurité

Confidentialité

garantit que les informations sont accessibles uniquement aux personnes autorisées. Cela implique l'utilisation de techniques de chiffrement et de contrôles d'accès pour empêcher l'accès non autorisé aux données.

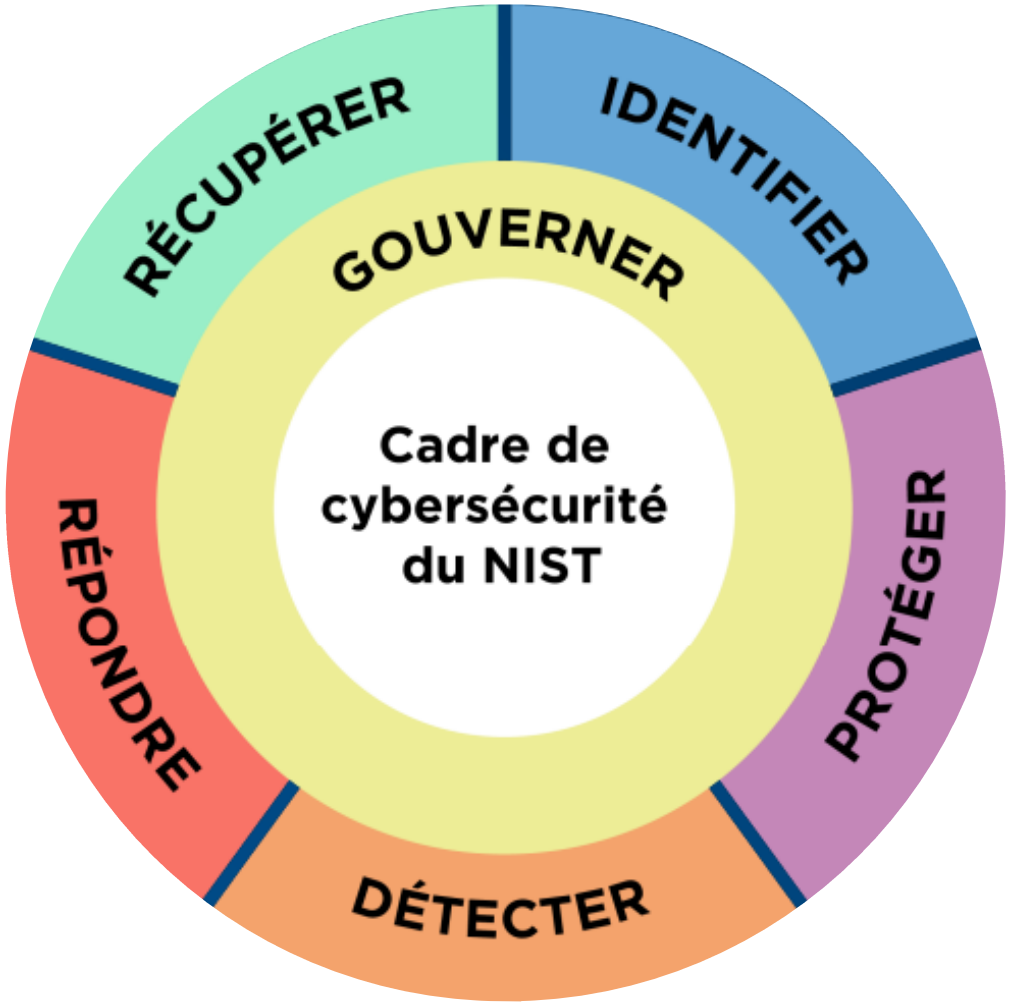
Intégrité

assure que les informations ne sont pas altérées ou modifiées de manière non autorisée. Cela inclut la protection contre les attaques qui pourraient corrompre les données, comme les ransomwares.

Disponibilité

garantit que les systèmes et les données sont accessibles lorsque nécessaire. Cela implique la mise en place de mesures pour prévenir les interruptions de service, comme les attaques par déni de service (DDOS).

Piliers d’un programme de cybersécurité en entreprise (NIST)



Principe	Composants
Gouverner	• Comprendre les besoins cyber • Élaborer une stratégie adaptée • Établir les politiques • Développer les et communiquer les pratiques • Mettre en place la gestion des risques de la chaine d’approvisionnement • Mettre en place la surveillance continue
Identifier	• Identifier les actifs critiques et inventorier les systèmes • Documenter les flux • Identifier les menaces et vulnérabilités • Identifier les améliorations à apporter
Protéger	• Former les utilisateurs • Protéger et surveiller les appareils • Protéger les données sensibles • Gérer et entretenir les logiciels • Sauvegarder l’information
Détecter	• Surveiller les réseaux et systèmes pour détecter les événements néfastes • Déterminer l’impact et la portée des éléments indésirables • Fournir des informations sur les événements indésirables au personnel et aux outils
Répondre	• Mettre en œuvre un plan d’intervention en cas d’incident • Classer les incidents • Collecter les données sur les incidents • Notifier les parties tierces • Contenir et éradiquer les incidents
Récupérer	• Comprendre les rôles et responsabilités • Exécuter le plan de reprise • Vérifier deux fois les éléments de récupération avant de les restaurer • Communiquer à l’interne et à l’externe

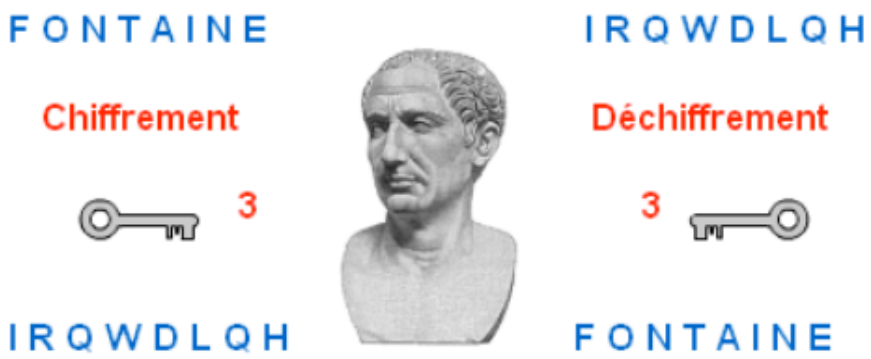
Le chiffrement, un concept central en sécurité des TI (1/2)

La cryptologie, ou science du chiffrement, est une pierre angulaire de la sécurité numérique moderne. Sans que nous nous en rendions compte, elle est omniprésente et essentielle pour protéger nos informations et garantir la confidentialité et l'intégrité des données. Ex.

- **VPN (« Réseau Privé Virtuel »)** : Sécurise les connexions internet pour travailler à distance.
- **Chiffrement des données** : Protège les informations stockées et en transit.
- **Sécurisation des réseaux** : Protège les communications entre appareils.
- **Signature électronique** : Garantit l'authenticité des documents signés, mais aussi sous-tend nombre de technologies fondamentales telles que l'authentification informatique ou les transactions carte de crédit.

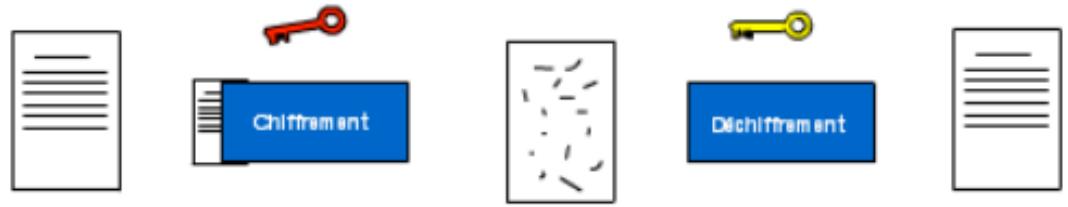
Le chiffrement, un concept central en sécurité des TI (2/2)
Concepts de base

Le chiffre de César (chiffrement symétrique)



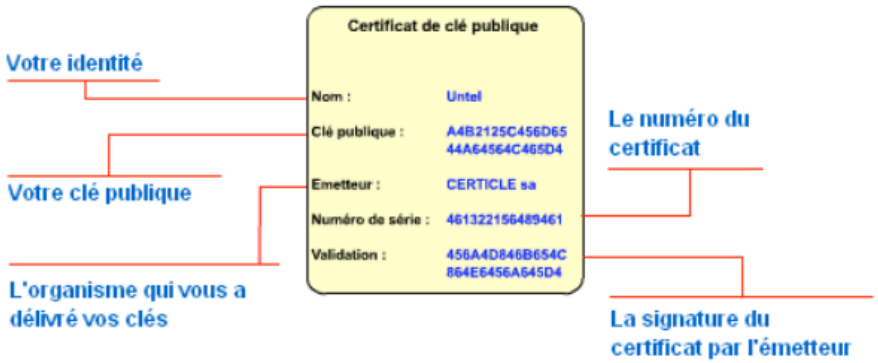
Source: ANSSI

Le chiffrement asymétrique



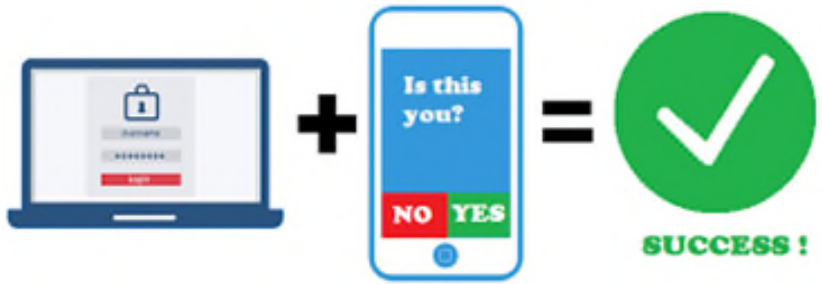
Source: ANSSI

Le certificat électronique



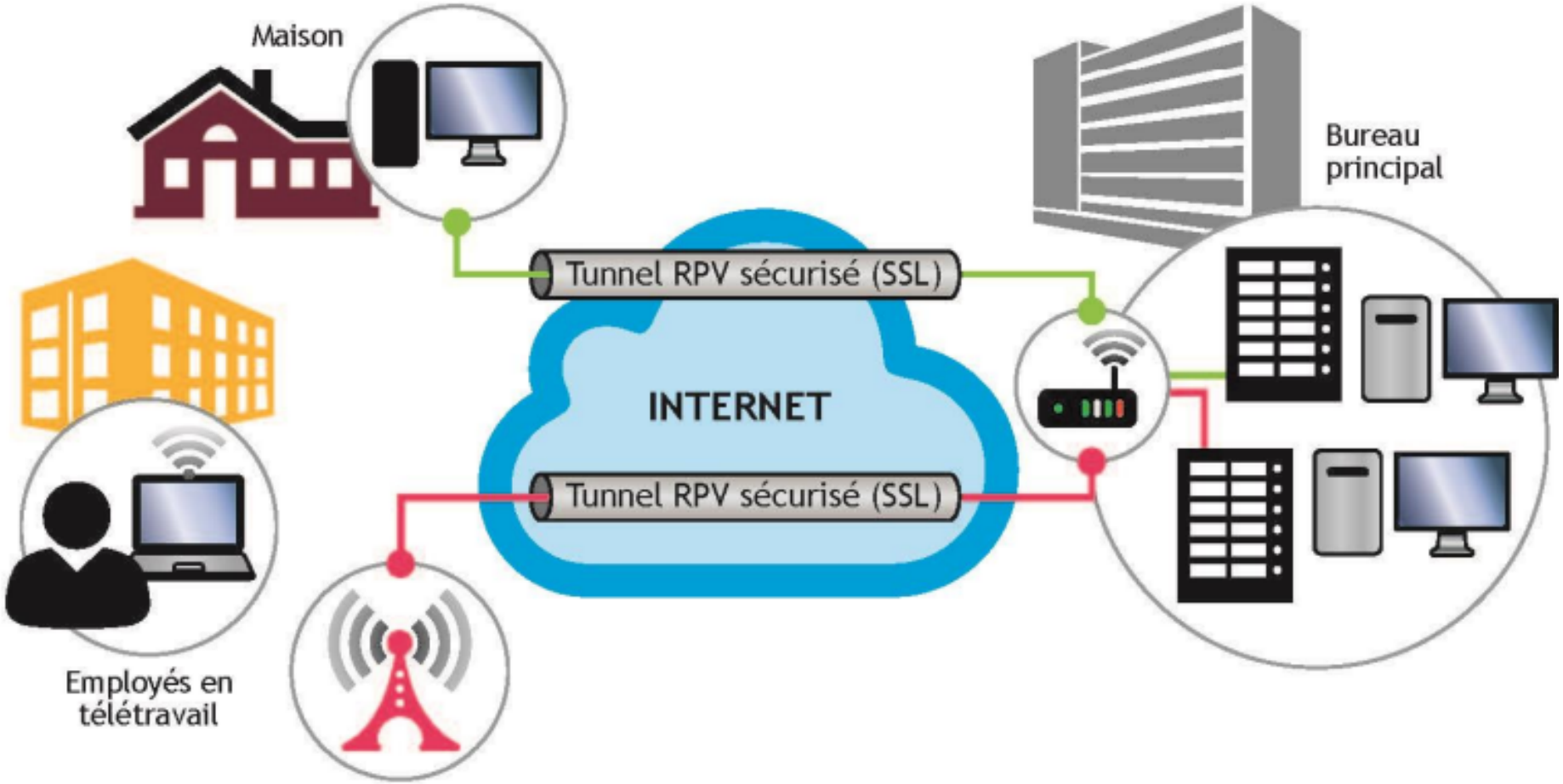
Source: ANSSI

L'authentification multi-facteurs (MFA)



Source: https://wellesleyps.org/

Le VPN pierre angulaire de l'architecture de sécurité en mode hybride



Source: Guide des TI du barreau du Québec

L’ingénierie sociale, danger exacerbé à l’heure de l’IA générative

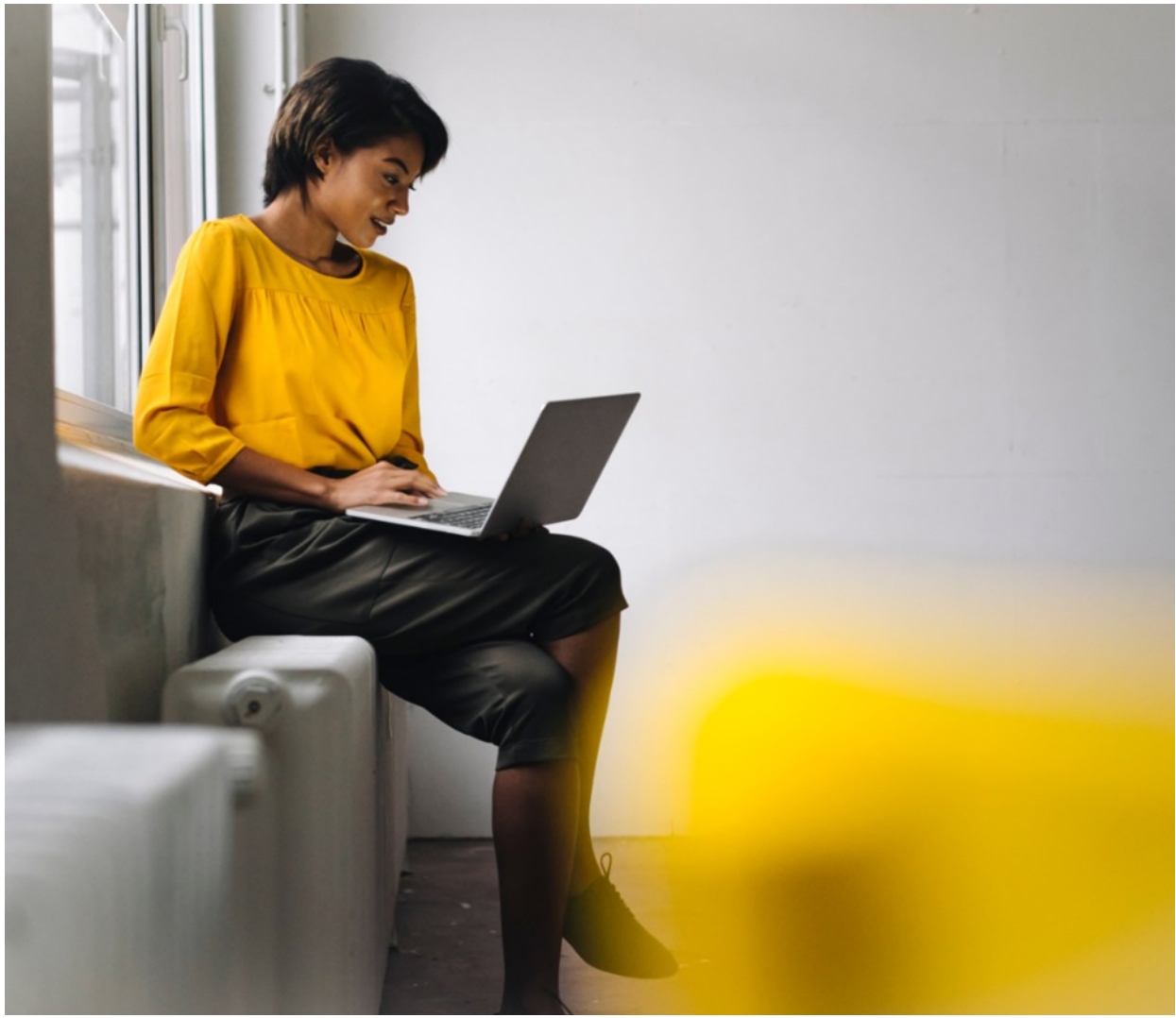
- **Phishing**: Envoi de messages trompeurs pour inciter la cible à effectuer une action, souvent via des liens ou pièces jointes malveillants. Le spear phishing cible spécifiquement un individu ou un petit groupe.
- **Business Email Compromise (BEC)**: L'attaquant se fait passer pour un cadre de l'organisation et demande un virement bancaire.
- **Fraude à la facture**: Les cybercriminels se font passer pour des vendeurs ou fournisseurs et envoient de fausses factures pour voler de l'argent.
- **Usurpation d'identité**: Les hameçonneurs se font passer pour des marques connues (DHL, LinkedIn, etc.) et incitent la cible à fournir ses informations d'identification.
- **Chasse à la baleine**: Attaques de spear phishing ciblant des employés de haut niveau, comme les dirigeants et cadres supérieurs.
- **Appât**: Utilisation de prétextes gratuits ou désirables pour inciter la cible à fournir ses identifiants ou à entreprendre d'autres actions.
- **Vishing**: Hameçonnage vocal réalisé par téléphone, utilisant des techniques similaires au phishing.
- **Smishing**: Hameçonnage par messages SMS, de plus en plus courant avec l'utilisation des smartphones.
- **Prétextat**: Création de faux scénarios pour inciter la cible à envoyer de l'argent ou des informations sensibles.
- **Quid Pro Quo**: L'attaquant offre quelque chose en échange d'informations précieuses.
- **Tailgating/Piggybacking**: Techniques pour accéder à des zones sécurisées en suivant une personne à travers une porte.

Source: Checkpoint

Mesures individuelles

Sécurité des accès, des sessions et des communications

- Verrouillez votre session de travail sur PC (Windows+L ou CMD+L) et activez le verrouillage automatique sur vos appareils mobiles.
- Utilisez un filtre de sécurité dans les espaces publics.
- Évitez les discussions confidentielles en public, que ce soit en personne ou par téléphone.
- Déconnectez-vous des sessions inactives et verrouillez votre poste.
- Activez votre pare-feu et votre VPN.
- Évitez les réseaux WIFI publics, préférez le partage de connexion mobile.
- Soyez prudent quant à vos publications sur les réseaux sociaux.
- Optez pour le stockage infonuagique au lieu du stockage local, en respectant les politiques de votre entreprise.
- Révisez les droits d'accès aux informations
- N'utilisez pas d'applications infonuagiques gratuites
- Définissez et documentez la méthode de communication avec le client.



Source: Guide des TI du barreau du Québec, Code de déontologie, Loi concernant le cadre juridique des technologies de l'information, PwC

Sécurité des accès, des sessions et des communications (suite)

- Relisez toujours les destinataires d’un courriel avant l’envoi.
- Utilisez le chiffrement et les étiquettes de messagerie quand c'est possible.
- Préférez les espaces de travail partagés (Teams, SharePoint, Google Drive) pour partager des liens au lieu de pièces jointes.
- Chiffrez les documents Word, Excel, PDF, etc. avec un mot de passe et communiquez-le par un autre moyen au client.
- Supprimez les métadonnées avant de partager des documents et soyez vigilant sur les pieds de page.
- Évitez de consulter des informations confidentielles envoyées par erreur.
- Effacez votre liste d’attente d’impression sur les imprimantes.

Source: Guide des TI du barreau du Québec, Code de déontologie, Loi concernant le cadre juridique des technologies de l’information, PwC

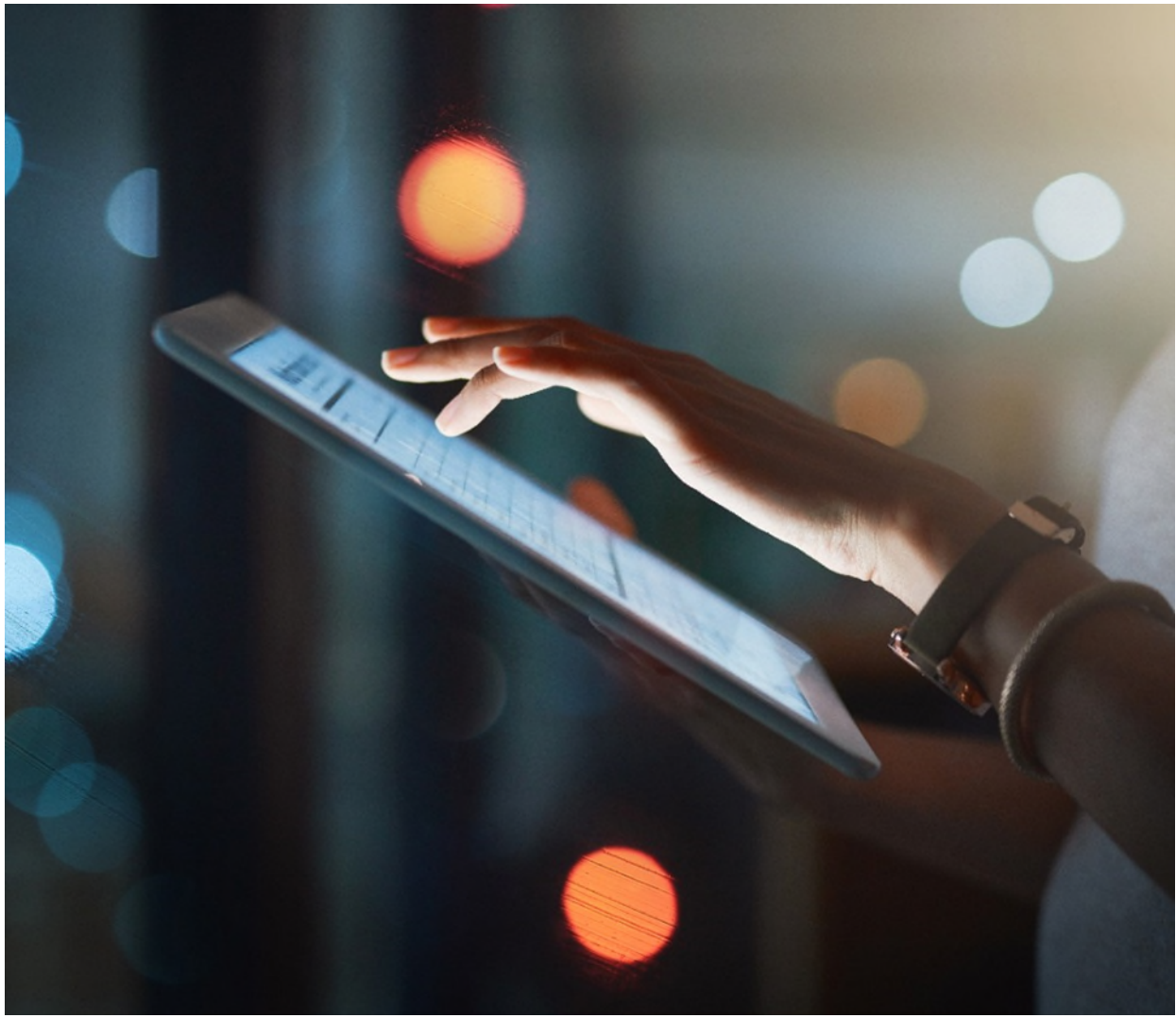
Gestion des mots de passe et authentification

- Modifiez régulièrement votre mot de passe et choisissez des mots de passe forts et uniques pour chaque compte.
- Activez l'authentification multifactorielle et utilisez un gestionnaire de mots de passe lorsque cela est possible.

Source: Guide des TI du barreau du Québec, Code de déontologie, Loi concernant le cadre juridique des technologies de l'information, PwC

Sécurité physique et gestion des documents

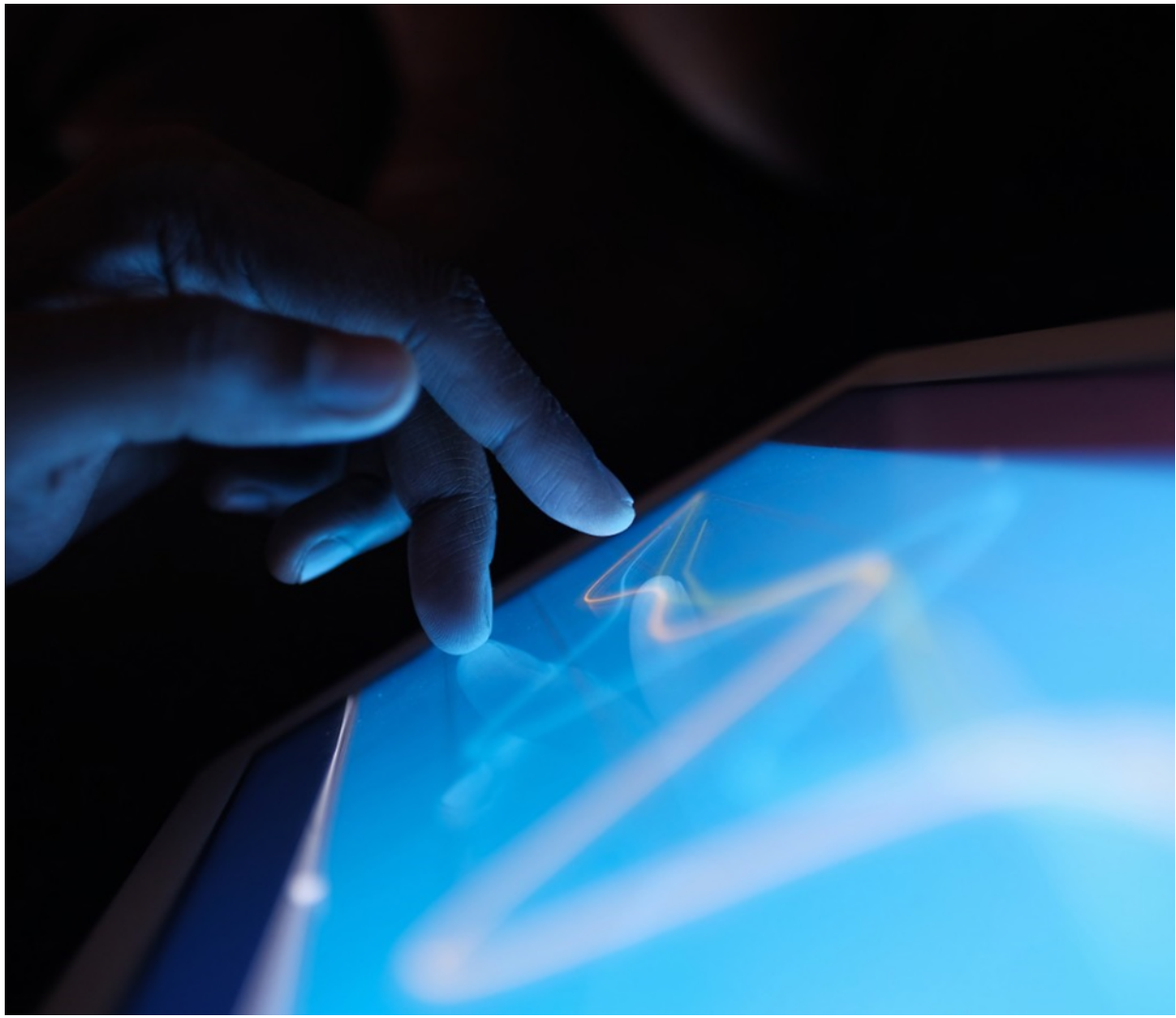
- Garder les documents physiques et les ordinateurs verrouillés, en suivant les politiques de sécurité (ne pas prêter les badges, effacer les tableaux, détruire les documents, etc.).
- Éviter l'utilisation de clés USB non identifiées.
- Nettoyer les documents physiques et numériques en supprimant ceux qui ne sont plus nécessaires.
- Ne pas quitter une entreprise avec des informations confidentielles.



Source: Guide des TI du barreau du Québec, Code de déontologie, Loi concernant le cadre juridique des technologies de l'information, PwC

Formation et BYOD

- S'informer et assimiler les politiques de sécurité de l'organisation (protection des données, étiquetage, utilisation acceptable des technologies, etc.).
- Maintenir votre antivirus à jour régulièrement.
- Respecter les directives de l'entreprise en matière de BYOD.
- Utiliser des comptes professionnels et éviter d'échanger des informations sensibles via des comptes personnels (par exemple, des groupes Messenger, WhatsApp, etc.).



Source: Guide des TI du barreau du Québec, Code de déontologie, Loi concernant le cadre juridique des technologies de l'information, PwC

2

Protection des renseignements personnels

Concepts clés

Loi 25: des impacts majeurs

Cette réglementation impacte toutes les organisations québécoises, qu'elles soient publiques ou privées, tant qu'elles gèrent des informations personnelles (clients, employés), à des fins internes ou externes

Les organisations sont-elles prêtes à se conformer ?

69%

expriment le besoin d'une plus grande clarté concernant les exigences pratiques de la Loi 25.

67%

signalent une préoccupation concernant le risque de pénalités et de sanctions pour non-conformité à la Loi 25.

52%

indiquent qu'ils manquent de ressources pour mettre en œuvre les exigences de la Loi 25.

Source: Gowling WLG, IAB Canada, Août 2023

Les organisations doivent opérer des changements majeurs:

- Gouvernance: normes, organisation, rôles et processus
- Droits des individus: accès, rectification, portabilité
- Vie privée dès la conception
- Remédiation de la conformité des activités existantes
- Transparence sur l'utilisation des informations personnelles
- Contrôle des transferts de données entre provinces, tiers, partenaires et sous-traitants
- Minimisation, suppression et anonymisation des informations personnelles
- Gestion des incidents: surveillance, signalement, remédiation

Facteurs clés de changement:

Gouvernance des données

Découverte des données

Protection des données

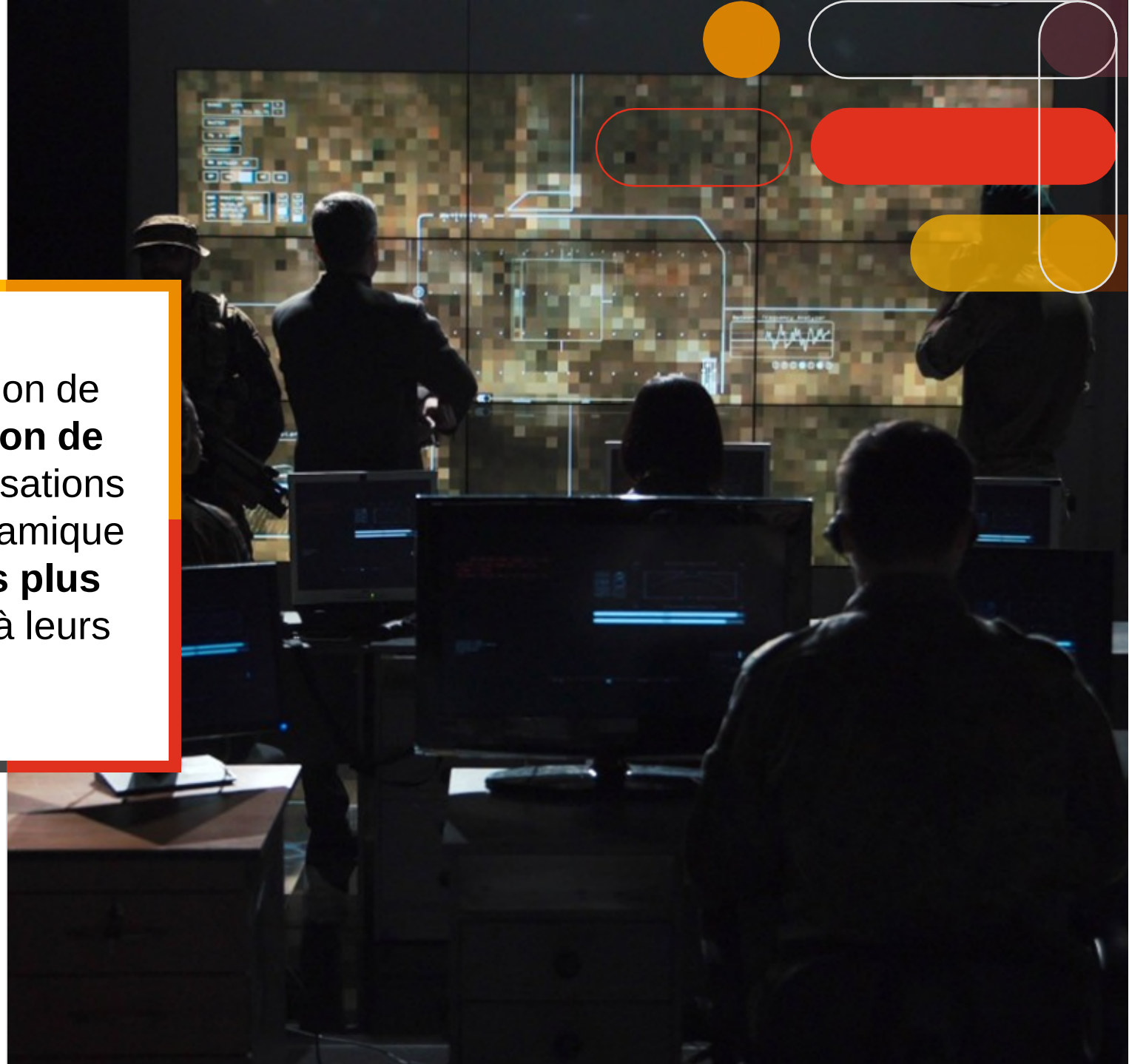
Minimisation des données

PwC Data Trust Framework

Article PwC:

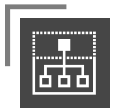
Bill 25: Are businesses ready for major changes in Quebec? By Jordan Prokopy

Avec le nouveau contexte de protection de la vie privée façonné par **l'introduction de la loi 25**, que font les grandes organisations pour **briser l'inertie** et obtenir la dynamique nécessaire pour **rendre les données plus accessibles** aux unités d’affaires et à leurs utilisateurs ?



Les organisations directement en contact avec la clientèle priorisent les domaines ayant le plus d'impact

Principaux thèmes observés: Les **domaines** énumérés ci-dessous présentent des **défis de mise en œuvre spécifiques** pour des grandes/anciennes organisations ayant des problèmes de données « Legacy » et nécessitant des **ressources importantes, une planification minutieuse et des plans de maintenance continus** pour assurer une mise en conformité efficace.



Gestion du consentement

Requis: prouver le consentement éclairé au traitement des RPs (et/ou identifier les cas où le traitement est exempté)

Défis: consensus stratégique, centraliser les informations, mettre en place des mécanismes de dépersonnalisation/anonymisation

Droits des personnes

Requis: répondre aux demandes de droits des personnes dans un délai de 30 jours (accès, rectification, objection, explication de la décision automatisée)

Défis: coordonner une réponse multidisciplinaire, trouver l'équilibre entre l'automatisation et les efforts manuels

Vie privée dès la conception et ÉFVPs*

Requis: évaluer les risques en matière de la vie privée et créer des produits conformes dès leur conception

Défis: identifier des déclencheurs appropriés, éviter les goulets d'étranglement et les reprises de travail, consensus sur les responsabilités

Gestion des incidents de confidentialité

Requis: confiner, enregistrer et déclarer les incidents de confidentialité au régulateur dans les plus brefs délais

Défis: détecter et qualifier les atteintes à la vie privée, faciliter la prise de décision multidisciplinaire

Gouvernance

Requis: établir et mettre en œuvre des politiques et des pratiques de gouvernance afin d'assurer la protection des RPs

Défis: mettre en place une gouvernance horizontale durable et efficace en termes de ressources, attribuer et former les ressources des affaires et des TI

Inventaire de traitements

Requis: démontrer la responsabilité en matière de protection de la vie privée, prouver que toutes les finalités de traitement sont établies avant la collecte des RPs

Défis: mobiliser les ressources pour les efforts de lancement initiaux, consensus sur les responsabilités

*Évaluations des facteurs relatifs à la vie privée

Les organisations affrontent ces défis de manière structurée, que nous regroupons en 4 étapes claires

Établir un mandat basé sur le risque et la stratégie

La première étape pour permettre un traitement sûr des données consiste à évaluer les écarts actuels par rapport à la loi, aux bonnes pratiques et aux attentes du public, ainsi que dans le contexte des **orientations stratégiques de l'organisation**.

Établir un modèle opérationnel cible pour le programme de protection de la vie privée

Les organisations visent ensuite à établir leur **modèle opérationnel cible** pour assurer un encadrement multidisciplinaire et gérer les impacts sur le fonctionnement habituel. Cela implique la **collaboration** entre les équipes de la protection de la vie privée, des unités d'affaires, des TI, de la gouvernance des données et de la sécurité.

Mettre en place un projet ciblé pour établir le modèle opérationnel cible

L'étape suivante consiste à mettre en place un projet pour établir un **programme intégré et discipliné**. Veiller à ce que le projet bénéficie d'un appui, d'une gouvernance et d'une expertise en la matière appropriés, et piloter le plan à l'aide d'actions, de calendriers et de budgets clairs.

Établir un outillage technologique évolutif en l'améliorant au fil du temps

La dernière étape consiste à doter le cadre organisationnel d'un outillage **technologique évolutif**. Cela permet de s'assurer que les processus de protection de la vie privée, tels que la gestion de l'inventaire et les EFVPs, sont maintenus de manière efficace en tirant parti des technologies d'industrialisation.

Mesures d’entreprise

To do list

Les informations présentées ici sont issues du Guide pratique pour la protection des renseignements personnels par l'avocat et son équipe (lien) édité par le barreau du Québec en 2023 en collaboration avec Me Antoine Guilmain

Principe	Contrôle
Personne responsable de la protection des renseignements personnels	• Nommer un responsable de la PRP par délégation de la plus haute autorité • Formaliser le rôle • Publier les coordonnées sur le site internet
Règles de gouvernance à l'égard des renseignements personnels	• Documenter les politiques et processus de protection des RPs, encadrant notamment a collecte, l'utilisation, le transfert, la conservation et la destruction des données personnelles, y compris celles concernant les mineurs. • Définir les rôles et responsabilités du personnel tout au long du cycle de vie des données, • Prévoir un processus de traitement des plaintes et gérer l'utilisation des cookies, tout en respectant les réglementations déontologiques et professionnelles. • Publier une version publique des politiques sur le site internet fournissant des informations claires et détaillées présentées de manière simple pour faciliter la compréhension par les clients.

Protection de la vie privée, liste de contrôle du barreau

Principe	Contrôle
Formulaires de consentement Lien vers les lignes directrices consentement de la CAI	• Cartographier les traitements des renseignements personnels. Identifier les RPs sensibles. • Inventorier les formulaires de consentement et s'assurer qu'ils respectent les exigences de la loi. • Fournir une information transaprente – fins auxquelles les renseignements personnels sont collectés et moyens par lesquels ils sont collectés; – droits d'accès, de rectification et de retrait du consentement ; – le cas échéant nom du tiers pour qui la collecte est fait – catégories des fournisseurs de services ayant accès aux renseignements personnels ; – transfert des renseignements à l'extérieur du Québec. • S'assurer qu'un consentement explicite est obtenu des individus concernés lorsque des renseignements personnels sensibles sont collectés.
Portabilité des données	• Déterminer si l'entreprise traite des RPs soumis au droit à la portabilité • Établir une procédure et le cas échéant les moyens techniques.

Protection de la vie privée, liste de contrôle du barreau (suite)

Principe	Contrôle
Ententes écrites	• Recenser les fournisseurs de services traitant des RPs • Privilégiez les fournisseurs au Québec ou établissez une EFVP pour déterminer les conditions du transfert et adapter les requis contractuels • Mettez à jour les contrats existants et négociez les nouveaux via des clauses standard.
Évaluation des facteurs relatifs à la vie privée Lien vers le guide EFVP de la CAI	• Effectuez une Evaluation de Facteurs Relatifs à la Vie Privée en cas de transfert hors Québec ou lors de la création de nouveaux traitements de renseignements personnels.
Politique de protection des renseignements personnels pour les employés	• Adopter ou mettre à jour une politique de protection des renseignements personnels pour les employés du cabinet. • Réviser les modèles de contrats de travail existants, en particulier les clauses de confidentialité, pour répondre aux exigences de protection de la vie privée.
Sensibilisation et formation	• Développer un programme de formation sur les règles relatives à la protection des renseignements personnels pour les employés qui traitent ou qui ont accès à des renseignements personnels. • Organiser des séances de formation annuelles sur les meilleures pratiques en matière de cybersécurité et de protection des données pour tous les membres du personnel du cabinet.

Protection de la vie privée, liste de contrôle du barreau (suite)

Principe	Contrôle
Incidents de confidentialité	• Établir une grille pour déterminer si un incident de confidentialité présente un risque de préjudice sérieux, et notifier la CAI et les personnes concernées si nécessaire. • Créer et maintenir un registre de tous les incidents de confidentialité, même sans risque de préjudice sérieux, et le conserver pendant au moins cinq ans.
Mesures de sécurité	• Les cabinets d'avocats ont une obligation générale de prendre les mesures de sécurité appropriées et raisonnables pour protéger les renseignements personnels qu'ils détiennent. • Mettre à jour le plan de réponse aux incidents de sécurité du cabinet et faire tester et approuver ce plan par des experts en cybersécurité. • Revoir la police d'assurance responsabilité du cabinet pour déterminer si les incidents de sécurité sont couverts. À défaut, évaluer souscrire à une police d'assurance couvrant ces risques. • Rappelons que les cyberrisques ne sont pas couverts par la police émise par le FARPBQ (Praeventio, février 2022). Vous pouvez consulter la police d'assurance responsabilité profession-nelle sur le site Internet du FARPBQ.

Protection de la vie privée, liste de contrôle du barreau (suite)

Principe	Contrôle
Confidentialité par défaut	• Déterminer si le cabinet utilise des technologies pour profiler, localiser ou identifier des individus, comme les témoins de connexion sur le site Internet. • Informer les individus de l'utilisation de ces technologies et des moyens d'activer la fonction au moment de la collecte. • Déterminer si le cabinet offre des produits ou services technologiques au public qui recueillent des renseignements personnels et disposent de paramètres de confidentialité. • S'assurer que les paramètres de confidentialité de ces produits ou services sont ajustés pour être conformes à l'exigence de confidentialité par défaut.
Biométrie	• Déterminer si votre cabinet utilise ou prévoit d'utiliser un système biométrique pour vérifier l'identité des personnes. • Remplir et transmettre le formulaire de la CAI si nécessaire. • Établir des lignes directrices internes sur l'utilisation des systèmes biométriques en tenant compte des exigences de protection des données.

Partie 5

L’avenir de la profession juridique

Conclusion

Quel avenir pour la profession juridique?

Numérisez le QR ou utilisez le lien pour participer

https://forms.office.com/r/UZWhs7i84e

Copier le lien

0 réponse envoyée

Cette présentation vous a-t-elle donné le goût d'entreprendre des projets de transformation technologique au sein de votre...

Oui

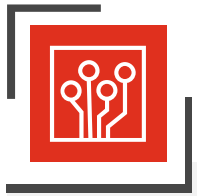
Non

Je ne suis pas certain

Carte proportionnelle | Barre

1 sur 1

Aspirer à pratiquer un leadership d'influence



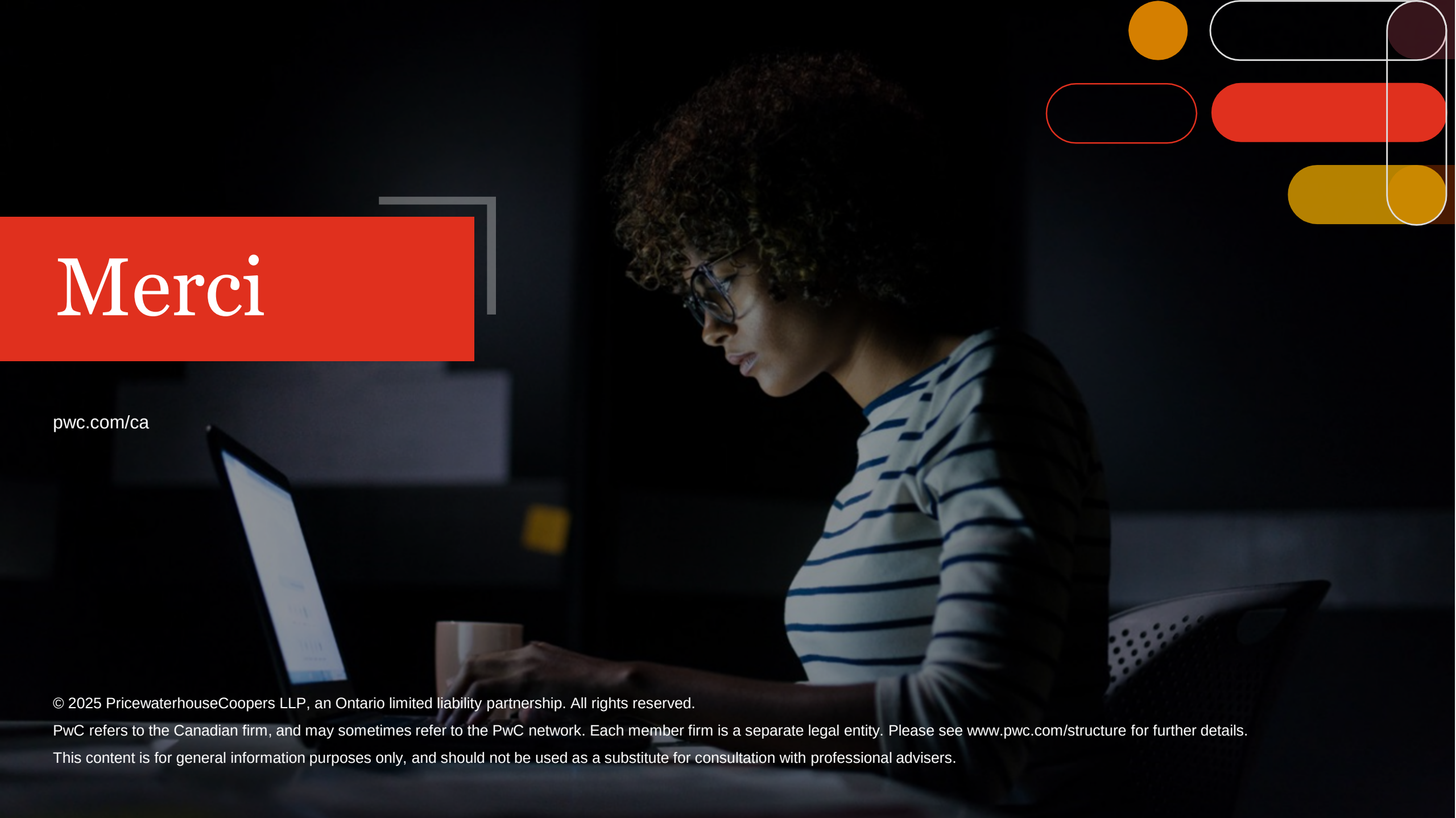
Comprendre la technologie

Évaluer les risques

Être proactif

Développer des politiques et procédures

Former et sensibiliser



Merci

pwc.com/ca