



10

Stagiaires et intelligence artificielle : opportunités, vigilance et encadrement par les maîtres de stage
Praktikanten und künstliche Intelligenz: Chancen, Prinzipien und Betreuung durch Praktikumsleiter

13

Est-ce une bonne idée pour les avocats d'utiliser l'intelligence artificielle dans leur marketing ?
Ist es eine gute Idee für Anwälte, künstliche Intelligenz in ihrem Marketing einzusetzen?

16

Les journalistes de la RTBF face à l'essor de l'intelligence artificielle
Die Journalisten des RTBF und der Einzug der künstlichen Intelligenz



Numéro spécial IA



LES CODES LARCIER

NOUVELLE
ÉDITION
DISPONIBLE
EN JUIN
2025



**BÉNÉFICIEZ DE L'ENSEMBLE DES DISPOSITIONS
LÉGISLATIVES ET RÉGLEMENTAIRES USUELLES EN BELGIQUE**

TOMES DISPONIBLES :

- Tome I Droit civil et judiciaire
- Tome II Droit pénal
- Tome III Droit de l'entreprise, de l'économie et de la finance (2 vol.)
- Tome IV Droit social (2 vol.)
- Tome V Droit fiscal
- Tome VI Droit public et administratif (2 vol.)
- Tome VII Droit de l'environnement
- Tables générales



APP LARCIER CODE

- > MISE À JOUR HEBDOMADAIRE DE L'ENSEMBLE DES TEXTES PRÉSENTS DANS VOTRE CODE
- > ACCESSIBLE DEPUIS VOTRE SMARTPHONE ET TABLETTE (VERSIONS IOS ET ANDROID DISPONIBLES)
- > VOS TEXTES LÉGISLATIFS DISPONIBLES ONLINE ET OFFLINE
- > ACCÈS SIMPLE ET PRATIQUE AUX ARTICLES GRÂCE AU MOTEUR DE RECHERCHE
- > ANNOTATIONS ACCESSIBLES ÉGALEMENT SUR L'APPLICATION



LARCIER
INTERSENTIA
LEFEBVRE GROUP

www.larcier-intersentia.com



Jean-François
Henrotte

Rédacteur en chef

<http://www.lexing.be/>

@Henrotte



INTELLIGENCE ARTIFICIELLE EN CABINET D'AVOCAT(E)S, ENTRE PRUDENCE ET NÉCESSAIRE INNOVATION

Künstliche Intelligenz in Anwaltskanzleien: Zwischen Vorsicht und notwendiger Innovation

Face à l'émergence rapide des technologies basées sur l'intelligence artificielle (IA), les cabinets d'avocat(e)s se trouvent à la croisée des chemins. Faut-il craindre l'IA ou l'embrasser ? Ce numéro spécial offre un éclairage essentiel sur les opportunités, mais aussi les précautions indispensables dans l'intégration de l'IA à la pratique juridique quotidienne.

Angesichts des raschen Aufkommens von Technologien basierend auf künstlicher Intelligenz (KI) befinden sich Anwaltskanzleien an einer Wegkreuzung. Sollte man KI fürchten oder sie annehmen? Diese Spezialausgabe bietet wichtige Einblicke in die Chancen, aber auch in die unerlässlichen Vorsichtsmaßnahmen bei der Integration von KI in die tägliche juristische Praxis

Comme l'indiquent Cynthia Charlier et Jeffrey Vigneron, les avocat(e)s doivent aujourd'hui composer avec un cadre réglementaire européen complexe, articulé autour du RGPD et de l'AI Act, qui imposent un encadrement strict, une supervision constante et une transparence irréprochable de l'usage de l'IA. Leurs grilles d'analyse vous y aident. Plus que jamais, il est crucial que les cabinets développent une réelle compétence technologique interne, sous peine de voir leur responsabilité juridique ou disciplinaire engagée.

Florence Garcet souligne pour sa part l'importance d'une utilisation éclairée de l'IA chez les jeunes avocat(e)s et stagiaires. Si ces outils constituent une aide précieuse, particulièrement

pour les tâches répétitives et chronophages, ils doivent impérativement être accompagnés par des chartes d'utilisation claires et des formations adéquates. En clair : l'avocat(e) de demain maîtrisera nécessairement l'IA, mais sans jamais perdre son sens critique ni son autonomie intellectuelle.

Sur un terrain différent, Joëlle Van Hecke nous rassure sur l'impact de l'IA dans les domaines administratifs et comptables des cabinets. Bien loin de remplacer les expert(e)s-comptables, l'IA leur permet de recentrer leur travail sur des missions à plus forte valeur ajoutée. Le traitement automatisé des factures, des paiements et la réduction des erreurs humaines

Éditorial

constituent autant de bénéfices immédiats et concrets.

Mais, comme le rappellent (l'omniprésent 😊) Jeffrey Vigneron et Axel Beelen, la cybersécurité doit être une préoccupation centrale. À l'heure de la directive NIS 2, les cabinets ne peuvent plus se permettre d'être les maillons faibles de la sécurité numérique. L'IA, certes utile, ne peut dispenser les cabinets de mettre en place une solide gouvernance en matière de cybersécurité, condition indispensable pour préserver la confiance de leurs client(e)s et partenaires.

Anne-Laure Losseau offre une réflexion nuancée sur l'utilisation de l'IA en matière de marketing. Tout en mettant en garde contre les dérives d'une communication trop artificielle, elle souligne judicieusement les bénéfices

pratiques que l'IA peut apporter : reformulation, brainstorming, traduction et création de supports visuels. Le succès réside dans une utilisation discrète et maîtrisée, semblable à une chirurgie esthétique réussie, où l'intervention ne doit pas sauter aux yeux.

Enfin, Aurélie Didier et votre serviteur complètent ce panorama en abordant respectivement les enjeux liés à la qualité éditoriale des contenus produits par l'IA et l'efficacité de celle-ci sur la traduction juridique. Nos contributions rappellent que l'humain, qu'il soit journaliste ou avocat(e), doit rester au cœur du processus pour garantir exactitude, fiabilité et authenticité des informations transmises.

En résumé, l'IA n'est ni amie ni ennemie : c'est un(e) partenaire exigeant(e), qui réclame vigilance, rigueur et responsabilité. Les cabinets

qui réussiront demain seront ceux qui sauront équilibrer innovation technologique et prudence déontologique. Bonne lecture !

Nous vous invitons également à lire l'article d'Alexandre Cassart, « Point sur l'évolution de l'IA au service des avocat(e)s & quelques exemples de prompt » (mis en ligne le 16 avril 2024, <https://ai-hub-fr.larcier-intersectia.com/ia-au-service-des-avocats>), accessible via le QR-code ci-dessous.





Cynthia Charlier

Avocat au barreau de Bruxelles et fondateur du cabinet Lawgitech



Jeffrey Vigneron

Avocat au barreau de Bruxelles et fondateur du cabinet Lawgitech

<https://lawgitech.eu>



L'INTÉGRATION DE L'INTELLIGENCE ARTIFICIELLE DANS LA PROFESSION D'AVOCAT : ENJEUX JURIDIQUES ET DÉONTOLOGIQUES

Die Integration von künstlicher Intelligenz in den Anwaltsberuf: rechtliche und deontologische Herausforderungen

Der Aufschwung der künstlichen Intelligenz im Rechtsbereich wirft für den Anwaltsberuf große Herausforderungen hinsichtlich der Einhaltung von Vorschriften, der Verantwortung und der Ethik auf. Um diesen Anforderungen gerecht zu werden, fußt der europäische Rechtsrahmen im Wesentlichen auf zwei Instrumenten: zum einen auf der DSGVO, die die personenbezogenen Daten der betroffenen Personen schützt, und zum anderen auf dem AI Act, der die Entwicklung und den Einsatz von KI-Systemen entsprechend ihrem Risikoniveau regelt. Diese beiden Verordnungen ergänzen und verknüpfen sich mit den nationalen berufsethischen Verpflichtungen, insbesondere den von Avocats.be und dem OVB erlassenen Standesregeln, sowie den internationalen ethischen Empfehlungen, um eine Grundlage für Anwälte zu bilden, die KI anwenden.

L'essor de l'intelligence artificielle dans le domaine juridique soulève des enjeux majeurs de conformité, de responsabilité et d'éthique pour la profession d'avocat. Pour y répondre, le cadre juridique européen repose essentiellement sur un dispositif double : d'une part, le

RGPD, protégeant les données à caractère personnel des personnes concernées ; d'autre part, l'AI Act, qui encadre spécifiquement le développement et l'utilisation des systèmes d'IA selon leur niveau de risque. Ces deux règlements se complètent et s'articulent

avec les obligations déontologiques nationales, notamment celles édictées par Avocats.be et l'OVB, ainsi que les recommandations éthiques internationales, pour former un socle cohérent de responsabilités à l'attention des avocats utilisateurs d'IA.

A. Cadre juridique européen : articulation entre AI Act et RGPD

L'intégration de l'intelligence artificielle (IA) dans la profession d'avocat repose sur une double assise juridique : d'une part, le droit de la protection des données personnelles, notamment le Règlement (UE) 2016/679 (RGPD), et, d'autre part, le Règlement (UE) 2024/1689 relatif à l'intelligence artificielle (AI Act), lequel encadre les obligations des acteurs en fonction de leur rôle dans la chaîne de valeur (fournisseur, déployeur, importateur, distributeur), des technologies mises en œuvre, ainsi que du niveau de risque associé à chaque système d'IA.

1. Un socle réglementaire européen double

Le Règlement (UE) 2024/1689 du 13 juin 2024, dit AI Act, établit un cadre juridique harmonisé applicable aux systèmes d'intelligence artificielle, définis comme des systèmes autonomes capables de générer des prédictions, recommandations ou décisions à partir de données en entrée. Il repose sur une approche graduée des risques, classifiant les systèmes d'IA selon leur niveau de dangerosité (articles 5 à 10). Il prévoit en outre un régime spécifique pour les modèles d'IA à usage général (General Purpose AI – GPAI), visés aux articles 51 à 56, et impose des exigences spécifiques en matière de transparence, de supervision humaine et de documentation technique (notamment les articles 14, 11 et 50).

Le Règlement (UE) 2016/679 du 27 avril 2016, dit RGPD, reste pleinement applicable à toute IA traitant des données à caractère personnel, tant lors de sa conception que de son exploitation (cf. considérants 10 et 70 de l'AI Act ; article 1^{er} RGPD).

Le RGPD et l'AI Act constituent deux instruments complémentaires : le premier assure la protection des droits fondamentaux des personnes physiques en matière de traitement de données à caractère personnel, tandis que le

second encadre le développement, la mise sur le marché et l'utilisation des systèmes d'intelligence artificielle, en particulier lorsque ceux-ci mobilisent de telles données.

2. Les obligations des avocats utilisateurs de systèmes d'IA

L'AI Act, adopté en juin 2024 et publié au *Journal officiel de l'Union européenne* en août, est entré en vigueur en septembre 2024. Conformément à son article 113, ses dispositions s'appliquent selon un calendrier progressif. *Depuis février 2025, les interdictions de certaines pratiques considérées comme présentant un risque inacceptable (article 5) sont pleinement effectives.* Les obligations applicables aux systèmes d'IA à haut risque (articles 6 à 29) entreront en vigueur courant 2026, tandis que les exigences spécifiques aux modèles d'IA à usage général, en particulier ceux présentant un risque systémique, seront mises en œuvre de manière échelonnée jusqu'en 2027. Dans ce contexte, *il est impératif d'anticiper dès à présent les implications de ce nouveau cadre réglementaire.* Les choix technologiques opérés aujourd'hui doivent intégrer les exigences futures afin de garantir une conformité durable et éviter des ajustements tardifs, souvent coûteux tant sur le plan économique que juridique.

L'AI Act désigne comme « déployeurs » (article 3, point 4) les entités, y compris les professions libérales, qui utilisent un système d'intelligence artificielle sous leur autorité dans le cadre de leur activité professionnelle. Cette définition englobe les cabinets d'avocats recourant à des outils d'IA dans l'exercice quotidien de leurs missions. Toutefois, les obligations qui en découlent varient en fonction de la nature du système d'IA utilisé et de son niveau de risque, tel que défini par la classification établie aux articles 5 à 10 du règlement.

a) Obligations générales applicables à tout usage d'IA

Dès qu'un avocat utilise un outil d'intelligence artificielle – qu'il s'agisse d'un outil de résumé de texte, de traduction, d'assistance à la rédaction ou de traitement automatisé de données – il doit respecter les obligations suivantes, qui s'appliquent quel que soit le niveau de risque du système :

- Licéité, loyauté et transparence du traitement des données. Toute utilisation d'un système d'IA impliquant des données à caractère personnel doit être fondée sur une base légale et respecter les principes généraux du RGPD (art. 5 et 6 RGPD).
- Minimisation des données et limitation des finalités. Les données traitées doivent être strictement nécessaires aux finalités poursuivies. Cela vaut également pour les outils IA en ligne (art. 5.1.c RGPD).
- Information des personnes concernées. Le client, ou toute personne concernée par un traitement de données via IA, doit être informé de façon claire et accessible (art. 13 et 14 RGPD).
- Facilitation de l'exercice des droits. L'avocat doit permettre l'exercice effectif des droits RGPD (accès, rectification, effacement, opposition, portabilité), même si les données sont utilisées pour entraîner ou interroger une IA (art. 15 à 21 RGPD).
- Supervision humaine. L'avocat doit toujours relire, valider et assumer le contenu produit ou suggéré par un système d'IA, même s'il ne s'agit pas d'une IA classée « à haut risque » (cf. art. 14 AI Act et principes déontologiques belges).

b) Obligations spécifiques aux systèmes d'IA à haut risque ou GPAI

Certaines obligations supplémentaires s'appliquent dès lors que l'avocat fait usage de :

Déontologie

- systèmes d'IA à haut risque (ex. : analyse automatisée de cas, génération de décisions ou de contrats sans supervision directe) ; ou
- modèle d'IA à usage général (GPAI) utilisés à des fins juridiques (type GPT-4 ou Claude dans des tâches complexes).

Dans ce cas, l'avocat doit également :

- Réaliser une analyse d'impact relative à la protection des données : conformément à l'article 35 du Règlement (UE) 2016/679 (RGPD), une telle analyse est obligatoire lorsqu'un traitement – notamment fondé sur un système d'IA – est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Cette exigence est également en cohérence avec les principes de gestion des risques et de sécurité prévus aux articles 9 et 27 de l'AI Act, ce dernier décrivant d'ailleurs le contenu d'une analyse d'impact qui concernant le déploiement de système d'IA à haut risque.
- Tenir une documentation technique complète et rigoureuse : l'article 13 de l'AI Act impose aux fournisseurs, et dans certains cas aux

déploieurs (notamment pour les systèmes à haut risque), d'assurer la traçabilité et l'explicabilité du système. Cette documentation doit couvrir, entre autres, la finalité d'usage, la nature et la provenance des données d'entrée, les résultats générés, ainsi que les mesures correctives ou d'atténuation mises en œuvre. L'article 26 précise les obligations incombant aux déploieurs de systèmes à haut risque.

- Mettre en place des mécanismes de remédiation et de suivi : en vertu des articles 14 (supervision humaine) et 26 de l'AI Act, il incombe aux déploieurs – y compris les professions réglementées comme les avocats – d'être en mesure de détecter des anomalies, d'interrompre l'usage du système ou d'en corriger les effets, notamment en cas d'atteinte aux droits fondamentaux.

B. Obligations déontologiques des avocats : lignes directrices d'Avocats.be et de l'OVB

Les lignes directrices conjointes de l'Ordre des barreaux francophones et germanophone (OBFG) et de l'Ordre des barreaux flamands

(OVB) (janvier 2025) posent un cadre déontologique structuré pour l'usage de l'intelligence artificielle (IA) par les avocats. Si l'usage de l'IA est reconnu comme relevant de la liberté professionnelle, il est assorti de conditions strictes engageant la responsabilité de l'avocat, tant sur le plan disciplinaire que juridique.

Les lignes directrices rappellent que le recours à l'intelligence artificielle relève de la liberté professionnelle de l'avocat. Toutefois, cette liberté s'accompagne d'une responsabilité certaine. L'usage de l'IA n'est ni prohibé, ni imposé, mais il doit être rigoureusement encadré : il doit faire l'objet d'une compréhension maîtrisée, d'une documentation appropriée et d'une supervision constante. Ces exigences valent y compris pour les outils ne relevant pas de la catégorie des « systèmes à haut risque » au sens du Règlement (UE) 2024/1689 (AI Act).

Les principales obligations sont les suivantes :

- Compétence technologique minimale : l'avocat doit comprendre le fonctionnement, les limites et les risques associés aux outils utilisés (art. 455 C. jud., art. 1.2 Codex OBFG).
- Supervision humaine obligatoire : il doit vérifier, corriger et assumer l'ensemble des contenus produits ou suggérés par l'IA. Il ne peut jamais déléguer intégralement une tâche intellectuelle ou stratégique à la machine.
- Protection des données et respect du secret professionnel : toute donnée introduite dans un outil d'intelligence artificielle doit, dans la mesure du possible, être pseudonymisée. L'avocat doit s'abstenir de renseigner des données à caractère personnel dans les prompts, champs de saisie ou documents transmis à des systèmes d'IA, en particulier lorsque ceux-ci sont accessibles en ligne. Pour renforcer la confidentialité, le recours à des solutions locales autonomes – telles que Ollama ou LM Studio – est recommandé. Bien qu'impliquant un traitement de données, ces solutions offrent un contrôle total sur



Déontologie

l'infrastructure, limitant ainsi les risques de fuite ou d'exploitation externe des données.

- Devoir de vérification et exigence de prudence : conformément aux obligations déontologiques en matière de compétence et de diligence, l'avocat doit vérifier systématiquement les contenus générés par un outil d'IA, qu'il s'agisse de références jurisprudentielles, doctrinales ou de raisonnements juridiques. Aucune confiance aveugle ne peut être accordée à l'IA : la relecture critique des résultats générés par l'IA est impérative, et l'avocat demeure pleinement responsable du contenu utilisé ou communiqué.
- Information du client et base légale du traitement : dans les cas où un traitement de données à caractère personnel via un outil d'IA s'avère nécessaire, l'avocat doit informer son client de manière claire et complète,

conformément aux articles 13 et 14 du RGPD, et, le cas échéant, obtenir un consentement éclairé. Cette obligation est particulièrement importante lorsque les données sont susceptibles d'être traitées par des prestataires tiers ou sur des infrastructures hors UE.

Contrairement au cadre européen issu de l'AI Act, qui repose sur une classification des systèmes d'intelligence artificielle en fonction de leur niveau de risque, les obligations déontologiques pesant sur les avocats s'appliquent de manière uniforme, quel que soit le type d'outil utilisé. Qu'il s'agisse :

- d'un assistant conversationnel généraliste (comme ChatGPT) ;
- d'un moteur de recherche juridique enrichi par l'IA (à l'instar de Genial) ; ou encore

- d'un modèle d'IA à usage général (GPAI) déployé localement sur les bases de données internes d'un cabinet,

l'avocat demeure tenu de respecter les mêmes exigences en matière de confidentialité, de vérification, de maîtrise technique et d'information du client.

Cela signifie que toute interaction avec un système d'IA, aussi banal ou peu intrusif soit-il, engage l'avocat. Ce dernier devient, de fait, responsable :

- de la qualité des résultats produits ;
- de la maîtrise des risques technologiques ;
- et de la protection des données personnelles éventuellement traitées.

Synthèse des obligations déontologiques des avocats en matière d'intelligence artificielle

 Thème	 Obligations déontologiques	 Références & détails
 Compétence technique	Comprendre les bases de l'IA et des LLMs ; former un jugement critique sur leurs résultats.	Art. 455 Code judiciaire / Codex OBFG – OVB
 Obligation de vérification	Vérifier les sources citées par l'IA (lois, jurisprudence, doctrine) ; analyser de façon critique les raisonnements proposés.	Pas de délégation du jugement professionnel
 Responsabilité	L'avocat demeure seul responsable des résultats utilisés ou communiqués via l'IA.	Principe de responsabilité non transférable
 Secret professionnel & confidentialité	Ne jamais introduire de données couvertes par le secret professionnel dans un outil IA sauf environnement fermé sécurisé. Privilégier la pseudonymisation.	RGPD art. 32 / AI Act art. 10 et 52 / Outils recommandés : Ollama, LM Studio
 Information du client	Si l'usage de l'IA impacte le conseil ou implique un traitement de données, le client doit être clairement informé.	RGPD art. 13-14 / Lignes directrices Avocats.be, OBFG
 Conditions d'utilisation	Lire attentivement les CGU et la charte privacy des outils IA : formation, stockage, traitements, localisation, droits de propriété.	Diligence requise avant usage
 Traitement de données personnelles	Éviter de renseigner des données personnelles dans les prompts sans consentement éclairé. Pseudonymisation recommandée.	RGPD art. 6, 9, 32, 35 / AI Act art. 29
 Transparence de l'usage	Aucune obligation générale de divulgation, sauf si le client interagit directement avec l'IA (ex. chatbot).	Pratique comparable aux autres outils informatiques / Recommandations UIA et OBFG



« Si un avocat utilise une IA pour traiter des données personnelles (par exemple, en résumant un dossier avec ChatGPT ou Claude), il reste responsable du respect des droits RGPD, même si la plateforme est tierce. »

C. Recommandations éthiques : CeSIA, CNIL

Face à l'émergence de systèmes d'intelligence artificielle (IA) dans les activités juridiques – qu'il s'agisse de rédaction, d'analyse, de prédiction ou d'interaction client – plusieurs institutions, en France, au Canada ou à l'échelle européenne, ont publié des recommandations éthiques structurantes. Ces lignes directrices n'ont pas valeur contraignante, mais elles traduisent un consensus professionnel sur les bonnes pratiques à adopter pour éviter des dérives, garantir le respect des droits fondamentaux, et assurer un usage maîtrisé de l'IA dans les professions du droit. Ces principes sont d'autant plus pertinents que la réglementation (AI Act, RGPD) n'encadre pas tout, en particulier les usages professionnels de systèmes considérés comme à « risque limité » ou « usage général », mais dont les effets peuvent être substantiels sur la qualité du conseil juridique, l'équité procédurale, ou le respect du secret professionnel.

1. CeSIA – Une vigilance éthique face aux risques systémiques

Le Comité d'éthique des systèmes d'IA (CeSIA), en France, identifie trois préoccupations majeures :

1. risques systémiques (hallucinations, erreurs massives, répliquabilité incontrôlée) ;

2. biais algorithmiques (notamment dans les IA entraînées sur des données non représentatives ou biaisées) ;
3. absence de supervision humaine, menant à une automatisation sans contrôle du raisonnement juridique.

Le CeSIA recommande aux professionnels – dont les avocats – de :

- pratiquer des audits réguliers de leurs outils IA (même internes) ;
- évaluer la traçabilité des décisions ;
- et anticiper les défaillances possibles, en gardant la capacité de désactiver ou abandonner un outil si nécessaire.

Exemple concret : un avocat qui confie à un assistant IA la rédaction d'un contrat doit être capable d'en expliquer chaque clause au client et de corriger une incohérence, même si elle provient du logiciel.

2. CNIL – Protéger les droits fondamentaux dans tout traitement IA

La CNIL insiste sur trois critères opérationnels :

- la clarté des finalités : l'avocat doit savoir *pourquoi* il utilise une IA (ex. : simplifier la recherche jurisprudentielle) et l'indiquer au client si nécessaire ;
- la proportionnalité des moyens : ne pas recourir à un outil complexe pour un usage

trivial, ou collecter plus de données que nécessaire ;

- et la garantie effective des droits : permettre l'accès, la rectification ou l'effacement des données, même après traitement via IA.

Cela signifie que si un avocat utilise une IA pour traiter des données personnelles (par exemple, en résumant un dossier avec ChatGPT ou Claude), il reste responsable du respect des droits RGPD, même si la plateforme est tierce.

D. Cas pratiques, usages concrets et outils : que peuvent faire les avocat(e)s, et à quelles conditions ?

L'intégration de l'intelligence artificielle dans les cabinets d'avocats ne se limite pas à une transformation technologique : elle implique une évaluation constante de la conformité aux règles déontologiques, au RGPD, et au Règlement (UE) 2024/1689 (AI Act). Trois cas emblématiques permettent d'illustrer les limites, tandis qu'une série d'outils concrets et licites permet d'envisager une utilisation professionnelle conforme.

Déontologie

1. Trois cas pratiques illustratifs : des enseignements pour la profession

Cas pratique	Nature de l'outil / Usage observé	Statut juridique (AI Act)	Usage possible par un avocat ?	Conditions et conséquences juridiques
COMPAS (États-Unis, 2016)	Prédiction du risque de récidive – biais algorithmiques démontrés (notamment raciaux)	Interdiction stricte (art. 5(1)(d) AI Act)	✗ Non	Usage interdit. L'avocat ne peut ni utiliser ni recommander ce type d'outil.
Klarna (Suède, 2024)	IA conversationnelle ayant remplacé 700 employés dans le service client	Usage possible – non à haut risque, mais soumis à supervision (art. 14 AI Act)	✔ Oui, sous conditions strictes	Usage limité à des fonctions non juridiques (tri, relances, FAQ). Relecture obligatoire. Information du client si l'IA influe sur le dossier. Aucune délégation du raisonnement juridique.

2. Usages concrets licites : l'IA comme « super-stagiaire », sous supervision

tâches juridiques ou administratives, à condition de respecter les principes de relecture, de sécurité et de conformité.

Les avocats peuvent utiliser des outils d'intelligence artificielle pour automatiser certaines

Tableau – Usages autorisés de l'IA par les avocats : outils, conditions, principes et références juridiques

Type d'usage	Outils recommandés	Conditions de licéité	Principes communs obligatoires	Références juridiques
🔍 Recherche juridique / analyse de jurisprudence	Predictice, Genial	Vérification manuelle Documentation du raisonnement Traçabilité des sources	Supervision humaine Contrôle des résultats Non-substitution du raisonnement Documentation des recherches	art. 14 AI Act Codex OBFG art. 1.2 RGPD art. 5, 6
🌐 Traduction / relecture de documents	DeepL Pro, Copilot pour juristes	Usage ponctuel Données pseudonymisées Relecture systématique	Confidentialité renforcée Aucune donnée sensible sans garantie Vérification du contenu généré	RGPD art. 25, 32 Codex OBFG art. 4.1
📝 Rédaction assistée / synthèse de dossiers	ChatGPT Enterprise, Claude Team	Hébergement sécurisé Relecture obligatoire Aucune délégation complète Données pseudonymisées	Supervision obligatoire Relecture et validation Responsabilité intégrale de l'avocat Conformité contractuelle de l'outil	Art. 14 AI Act RGPD art. 32 Codex OBFG art. 1.2
🛡️ Hébergement local / confidentialité renforcée	Ollama, LM Studio	Stockage interne maîtrisé Contrôle des flux Pas d'exposition externe des données sensibles	Secret professionnel garanti Pseudonymisation des données Auditabilité des systèmes locaux	RGPD art. 25, 32 Codex OBFG art. 4.1

Encadré complémentaire – Obligations transversales et niveaux de risque

- Ces principes communs s'appliquent à tous les usages d'IA, quel que soit le niveau de risque identifié par l'AI Act.
- L'avocat doit pouvoir démontrer qu'il a supervisé, vérifié et sécurisé l'usage de l'outil utilisé.
- En cas d'utilisation d'un système d'IA à haut risque ou d'un modèle d'IA à usage général (GPAI), des obligations supplémentaires s'imposent, conformément au cadre européen (cf. point A, 2, b).

Conclusion

L'avocat qui intègre l'intelligence artificielle dans sa pratique demeure en toutes circonstances responsable des choix technologiques qu'il opère et de leurs conséquences. Cette responsabilité est d'autant plus marquée lorsque l'outil utilisé relève d'un système d'IA à haut risque ou d'un modèle à usage général (GPAI) présentant un risque systémique, au sens du Règlement (UE) 2024/1689. Dans ces cas, le professionnel est tenu de respecter les obligations supplémentaires en matière de supervision humaine, de transparence, de documentation technique et d'évaluation des risques.

Les lignes directrices belges et internationales rappellent que cette responsabilité est personnelle, non délégable, et qu'aucun recours à l'IA – quelle que soit sa sophistication – ne peut justifier une défaillance dans le respect du secret professionnel, du devoir de vérification ou du devoir de diligence. *Il incombe à l'avocat de veiller à ce que l'usage qu'il fait de l'intelligence artificielle soit pleinement maîtrisé, techniquement traçable, juridiquement documenté, et strictement conforme tant aux exigences déontologiques de la profession qu'au cadre réglementaire européen applicable, notamment en matière de protection des données et de gestion des risques liés aux systèmes d'IA. À défaut, il pourrait engager sa responsabilité civile, voire disciplinaire, avec une intensité supérieure à celle applicable en cas d'usage de méthodes traditionnelles.*



Florence
Garcet

Avocate au barreau de
Liège-Huy

<https://be.linkedin.com/in/florence-garcet-7688206a>



STAGIAIRES ET INTELLIGENCE ARTIFICIELLE : OPPORTUNITÉS, VIGILANCE ET ENCADREMENT PAR LES MAÎTRES DE STAGE

Praktikanten und künstliche Intelligenz: Chancen, Prinzipien und Betreuung durch Praktikumsleiter

L'intelligence artificielle (IA) s'invite de plus en plus dans le monde du travail et nos cabinets d'avocat(e)s ne sont pas épargnés. Si certains confrères regardent encore l'IA avec méfiance, d'autres, souvent plus jeunes, y voient un outil d'une redoutable efficacité.

On peut légitimement penser que c'est le cas des stagiaires qui sont ce qu'on pourrait appeler des « digital natives ». L'IA générative peut modifier leurs méthodes de travail, parfois même sans que les maîtres de stage en soient conscients.

L'enjeu est réel, entre opportunité technologique et risques déontologiques, l'encadrement des usages de l'IA devient indispensable. Nous tentons d'émettre ici quelques pistes de réflexion.

Künstliche Intelligenz (KI) hält immer mehr Einzug in die Arbeitswelt und auch unsere Anwaltskanzleien bleiben davon nicht verschont. Während einige Kollegen die KI noch mit Misstrauen betrachten, sehen andere, oftmals jüngere Kollegen, in ihr ein Werkzeug von enormer Effizienz.

Man kann mit Recht davon ausgehen, dass dies bei Praktikanten der Fall ist, die man als „digital natives“ bezeichnen könnte. Die generative KI kann ihre Arbeitsmethoden verändern, manchmal sogar ohne dass sich die Praktikumsleiter dessen bewusst sind.

Es steht viel auf dem Spiel, zwischen technologischen Chancen und ethischen Risiken, und ein Rahmen für die Nutzung von KI wird unerlässlich. Wir versuchen hier, einige Denkanstöße zu geben.

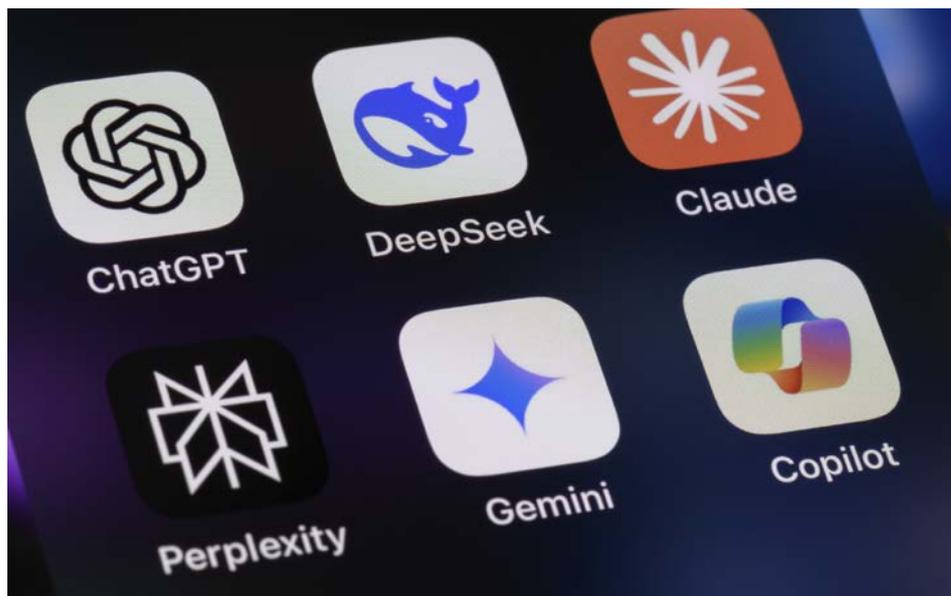
1. L'IA, un outil efficace pour jeunes (et moins jeunes) avocat(e)s

Il faut reconnaître que les outils d'intelligence artificielle (ChatGPT, Claude, Gemini, Perplexity...) peuvent offrir aux avocats une aide précieuse pour la réalisation de certaines

tâches juridiques, et notamment la rédaction de brouillons de conclusions, de notes, la reformulation de textes ou de contrats, la synthèse d'articles de doctrine ou de jurisprudence, l'élaboration de canevas de courriels, la création de présentations à destination de clients, etc.



« Le maître de stage a aujourd'hui une obligation de "formation technologique". »



Force est de constater que ce sont des tâches généralement confiées aux stagiaires.

S'il est évident que l'IA ne peut pas se substituer à l'analyse juridique humaine, il s'agit incontestablement d'une aide à la rédaction et à la structuration de la pensée. À notre estime, le plus grand challenge du stagiaire est tout d'abord de caractériser les faits et les questions juridiques d'un dossier ainsi que de choisir la stratégie à adopter. Si une discussion avec le maître de stage peut évidemment pallier cette difficulté, l'IA permet, elle aussi, de stimuler la créativité juridique. L'utilisation d'un outil d'IA peut ainsi servir de point de départ à la réflexion afin de surmonter la « page blanche » qui survient parfois à l'entame d'un dossier.

Lorsque l'outil d'IA est bien maîtrisé, il peut également permettre un gain de temps considérable pour des tâches dites répétitives et souvent chronophages.

Face à ce constat, on admettra que les stagiaires (comme tout avocat) ont intérêt à

maîtriser de tels outils afin d'améliorer la qualité et la rapidité de leur travail.

2. Risques déontologiques et juridiques

Si l'IA représente une belle opportunité pour l'avocat et le stagiaire, son usage n'est pas anodin. L'utilisation des outils d'IA fait naître une série de risques qu'il ne faut pas sous-estimer. Nous en citerons quelques-uns de manière non exhaustive :

– Confidentialité et secret professionnel

On le sait, les outils d'IA fonctionnent souvent sur des plateformes externes qui stockent les données et les réutilisent de manière peu transparente. Il existe un véritable risque que des données personnelles, voire des données sensibles, soient divulguées sur internet, sans aucune chance de les récupérer (ou de savoir à quelles fins elles sont utilisées). Injecter des données personnelles dans les outils d'IA sans vérification complémentaire quant aux mesures de confidentialité mises en place ou sans anonymisation revient à compromettre gravement

nos obligations de confidentialité et de secret professionnel.

Rappelons que les avocats sont également soumis au Règlement général sur la protection des données. En qualité de responsable de traitement, ou de sous-traitant dans le cas des stagiaires, les avocats doivent s'assurer d'utiliser des outils sécurisés et de respecter les principes du Règlement européen (transparence...).

– Fiabilité des réponses générées

L'IA générative est connue pour produire des contenus « plausibles », mais pas toujours exacts. On voit régulièrement des outils d'IA « halluciner », en créant par exemple des citations de jurisprudence qui n'existent pas. Si le stagiaire s'en remet aveuglément à l'outil (ou si le maître de stage se fie à un brouillon sans le relire attentivement), le *dominus litis* s'expose à des erreurs potentiellement préjudiciables.

Il est donc indispensable que le stagiaire maîtrise la matière qui a été soumise à l'IA et puisse vérifier activement les sources produites.

– Plagiat et propriété intellectuelle

Soulignons encore que l'IA peut générer des contenus et reproduire partiellement des textes protégés par des droits de propriété intellectuelle sans les citer. Cela soulève évidemment des questions juridiques, mais aussi éthiques.

3. Solutions pour diminuer les risques

Deux solutions sont, selon nous, à privilégier, à savoir, d'une part, l'adoption d'une charte d'utilisation de l'IA dans les cabinets d'avocats et, d'autre part, la formation des stagiaires à l'usage de l'intelligence artificielle.

3.1. Adoption d'une charte d'utilisation à l'IA dans le cabinet d'avocat(e)s

La charte ne doit pas être vue comme un frein, mais plutôt comme un guide qui permet

d'établir un cadre clair, adapté au cabinet, pour promouvoir une utilisation responsable des outils d'IA.

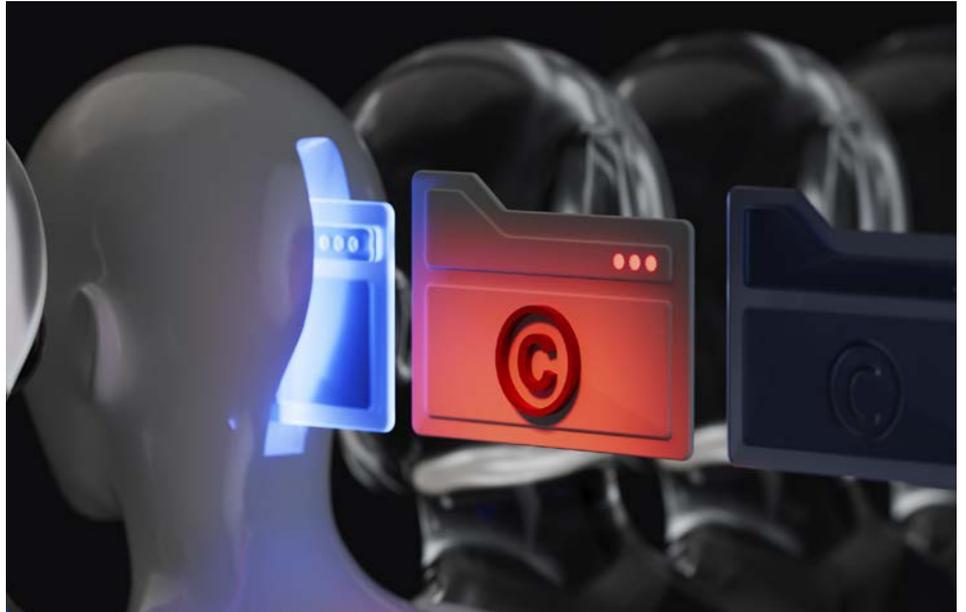
Nous recommandons de rédiger cette charte en s'inspirant des lignes directrices émises par Avocats.be et l'OVB en matière d'utilisation de l'intelligence artificielle par les avocats¹.

En pratique, on peut recommander d'insérer dans la charte les clauses suivantes :

- liste des outils autorisés ou interdits au sein du cabinet ;
- interdiction de soumettre à l'IA des documents contenant des données confidentielles non anonymisées ;
- obligation d'indiquer en interne lorsqu'un contenu a été rédigé avec l'aide d'une IA ;
- interdiction de « copier-coller » sans vérification humaine ;
- relecture obligatoire par un avocat pour tout contenu destiné à un client ou à une juridiction.

3.2. Formation et sensibilisation du et de la stagiaire

Une charte seule ne suffira cependant pas. Il est primordial d'accompagner les stagiaires (et tout avocat d'ailleurs) dans l'apprentissage des outils d'IA. Il nous semble que le maître de stage a aujourd'hui une obligation de « formation technologique » en plus des obligations de formations classiques.



Nombre de formations sont aujourd'hui proposées aux avocats pour leur permettre de comprendre au mieux les outils d'IA et à les utiliser efficacement. Les stagiaires ont également parfois des formations « IA » spécifiques à leur intention, comme c'est notamment le cas au Barreau de Liège-Huy dans le cadre d'un Séminaire « innovation ». On espère évidemment que ce type d'initiative tendra à se multiplier.

La formation du stagiaire ne s'étend pas selon nous uniquement à l'intelligence artificielle à proprement parler. Il est impératif de rappeler au stagiaire les principes fondamentaux en matière de protection des données, mais surtout de lui apprendre à penser de manière critique, à croiser les sources, vérifier les résultats, etc.

Notre conseil

L'IA ne remplacera pas les avocats, mais les avocats qui savent l'utiliser remplaceront peut-être ceux qui l'ignorent.

Pour nos stagiaires, les outils d'intelligence artificielle représentent à la fois des risques et des opportunités. Ils permettent d'aller plus vite, mais pas toujours plus juste. Il appartient aux maîtres de stage d'organiser leur usage, d'en expliquer les limites, et d'encourager une utilisation éclairée de ces nouvelles technologies.

1. www.ordevanvlaamsebalies.be/nl/fetch-asset?path=ovb/Documents/Digitalisering/Richtlijnen-voor-advocaten-voor-het-gebruik-van-Artifici%C3%ABle-Intelligentie.pdf.



Anne-Laure
Losseau

Executive and Career
Coach

[https://www.
aligncoaching.be/](https://www.aligncoaching.be/)

@Allousseau



EST-CE UNE BONNE IDÉE POUR LES AVOCATS D'UTILISER L'INTELLIGENCE ARTIFICIELLE DANS LEUR **MARKETING** ?

Ist es eine gute Idee für Anwälte, künstliche
Intelligenz in ihrem **Marketing** einzusetzen?

Nein, das ist meiner Meinung nach eine sehr schlechte Idee.

So oder so ähnlich lautete meine Antwort, als mir die Redaktionsleiterin vorschlug, diesen Beitrag zu verfassen, der von vornherein dazu bestimmt war, relativ „kurz“ zu sein.

Glücklicherweise beinhaltet diese Frage jedoch einen großen Spielraum für nuanciertere Betrachtungen.

Lassen Sie uns also einen genaueren Blick darauf werfen, ob und wie uns künstliche Intelligenz (auch generative Intelligenz, GI) im Marketing nützlich sein kann.

Non, c'est à mon avis une très mauvaise idée.

C'était, à peu de chose près, ma réponse lorsque la directrice éditoriale m'a proposé de rédiger cette contribution, qui était donc *a priori* vouée à être relativement « concise ». Je voyais défiler devant mes yeux les « posts », à l'accroche digne d'un magazine à sensation (le typique : « J'ai longuement hésité avant de vous parler de ceci... »), au contenu insipide mais accompagné d'un portrait flatteur du/de la prétendu/e auteur/trice (portrait de son bon profil et à l'éclairage parfait mais bien entendu toujours pris à son insu, tandis qu'il/elle était en pleine action/réflexion), le tout

dans un format soigneusement étudié et répliqué pour – censément – plaire à l'algorithme du réseau social.

Si elles parviennent, le cas échéant, à satisfaire l'algorithme, ces publications ont en tout cas le don de provoquer chez moi, vous l'aurez compris, une réaction épidermique de rejet. Il va sans dire que si j'avais à choisir un(e) avocat(e) pour me défendre, ce

genre de message me ferait fuir plus qu'autre chose.

Fort heureusement, la nuit porte conseil et permet parfois de nuancer des réactions par trop lapidaires.

Envisageons donc, en y regardant de plus près, si et comment l'intelligence artificielle (dite générative, IA) peut nous servir utilement en matière de marketing.



« Les textes générés par l'IA sont fluides et agréables à lire mais ils manquent précisément de ces aspérités qui touchent le lecteur, comme un choix de mots surprenant, une expression plus personnelle ou créative ou une référence "d'initiés". »

Ce qui fonctionne

Le but, lorsque l'on publie sur les réseaux sociaux (s'agissant de positionnement professionnel, je pense principalement à LinkedIn), est d'avoir une visibilité la plus étendue possible et beaucoup de réactions, de préférence positives.

De manière empirique et sans me prétendre experte en réseau social, il me semble que les ingrédients de beaucoup de publications qui « marchent » sont :

- une photo (de l'auteur/autrice) qui attire l'œil (oui c'est comme ça)
- un message qui provoque une émotion suffisamment puissante chez le lecteur/la lectrice, telle que de l'admiration (pour une réussite ou une démonstration de son expertise), un élan de compassion/sympathie, de l'indignation face à une situation ou encore

une identification/résonance forte avec le message véhiculé.

Les textes générés par l'IA sont fluides et agréables à lire mais ils manquent précisément de ces aspérités qui touchent le lecteur, comme un choix de mots surprenant, une expression plus personnelle ou créative ou une référence « d'initiés ».

Dans le pire des cas, ces textes sont aseptisés, stéréotypés et ils sonnent faux. Le plus souvent ils sont remplis de banalités, clichés et autres prêts-à-penser.

C'est d'ailleurs le même phénomène qui est à l'œuvre dans les lettres de motivations « *made by ChatGPT* », que les recruteurs ne lisent même plus : il y a fort à parier qu'elles disparaîtront dans un avenir proche pour cette raison.

Non seulement les textes générés par l'IA sonnent faux mais ils contiennent parfois des erreurs (les fameuses hallucinations). Gare, par exemple, aux erreurs de déontologie, comme « en tant qu'avocat, il nous est interdit de faire de la publicité ». C'est faux : la publicité, et même le démarchage, sont en Belgique autorisés depuis longtemps pour les avocats (moyennant bien entendu le respect des principes de dignité, délicatesse, probité et discrétion).

En tant que professionnel(le) (du droit), l'expertise reste le facteur-clé de la confiance et nous sommes toujours la meilleure personne pour en faire la démonstration.

Vous l'aurez compris, je n'aime pas les textes générés par l'IA et je n'ai pas encore parlé des images qu'elle produit, qui sont inesthétiques sinon carrément glauques. Même les plus réussies vous inspirent un désagréable sentiment de malaise.

En bref, les lecteurs ont besoin d'authenticité, de profondeur, de connexion avec la personne qui écrit, de professionnalisme et même d'aspérités : car c'est tout cela qui touche, qui inspire confiance et donne envie d'entrer en contact, de nous suivre ou de nous consulter.

Tout ce que l'IA peut faire pour nous

Après ce vibrant plaidoyer contre l'utilisation de l'IA, voici une liste (non exhaustive) de tâches pour lesquelles l'IA peut être un assistant de premier choix, en particulier dans nos démarches de « marketing ».



Marketing



Conclusion

Le marketing, c'est l'art de se faire connaître de son public et son maître-mot, en particulier pour un métier où *l'intuitu personae* est clé, c'est la création du lien.

On crée du lien par la démonstration de son expertise et la sincérité de ses propos. Rien ne nous empêche de nous aider de l'IA mais à condition de ne rien perdre de ce qui nous définit, nous singularise, nous rend unique (et hautement irrésistible).

La belle saison bat son plein et je conclurai donc par une comparaison de circonstance. L'IA est comme la chirurgie esthétique : pour que le résultat soit réussi, il faut qu'elle ne saute pas aux yeux.

1. L'IA est un as pour reformuler une idée confuse.
Il arrive qu'une idée, pourtant claire dans notre esprit, ne prenne pas forme : l'IA peut transformer nos ébauches en formules intelligibles.
2. L'IA est un excellent partenaire de « brainstorming ».
Lorsque nous sommes paralysés par l'angoisse de la page blanche, l'IA nous proposera volontiers des idées et les affinera à volonté et sans jamais se plaindre au fil d'un échange de type « brainstorming ».
3. L'IA permet d'élargir notre audience grâce à des traductions de grande qualité.
Rien de plus simple, si nous voulons partager nos idées en néerlandais ou en anglais par exemple, que de les faire traduire en quelques secondes par l'IA (DeepL est l'outil le plus connu).
4. L'IA peut rendre nos idées plus percutantes grâce à des supports visuels.
L'IA nous assistera très avantageusement pour exprimer visuellement nos idées sous la forme de graphiques, schémas, tableaux et autres supports.
5. L'IA transforme les données brutes en informations.
L'IA peut nous aider à mesurer et interpréter, par exemple, l'impact de publications et démarches de marketing (comportement de fréquentation de notre site, de notre profil, etc.).



Aurélie Didier

Journaliste
Directrice éditoriale
adjointe de l'information
et des sports à la RTBF

<https://www.linkedin.com/in/aur%C3%A9lie-didier/>



LES JOURNALISTES DE LA RTBF FACE À L'ESSOR DE L'INTELLIGENCE ARTIFICIELLE

Die Journalisten des RTBF und der Einzug der künstlichen Intelligenz

Aujourd'hui la rédaction de la RTBF teste et utilise plusieurs outils d'intelligence artificielle en se basant sur des balises à respecter. Le média de service public veut intégrer l'IA pour automatiser des tâches à faible valeur ajoutée. Cela permet d'une part aux journalistes de se concentrer sur des activités à plus haute valeur ajoutée et d'autre part à la rédaction d'élargir sa capacité d'informer le public. Il est nécessaire pour la RTBF de trouver un équilibre entre l'IA et l'humain pour préserver l'essence du métier de journaliste et la confiance du public.

Mittlerweile testet und verwendet die Redaktion des RTBF mehrere KI-Tools. Das öffentlich-rechtliche Medium will KI integrieren, um Aufgaben mit geringer Wertschöpfung zu automatisieren. Dadurch können sich einerseits die Journalisten auf Tätigkeiten mit höherer Wertschöpfung konzentrieren und andererseits kann die Redaktion ihre Fähigkeit, die Öffentlichkeit zu informieren, erweitern. Es wird notwendig sein, ein Gleichgewicht zwischen KI und menschlichem Output zu finden, um das Wesen des Journalistenberufs und das Vertrauen der Öffentlichkeit zu bewahren.

Les journalistes vont-ils progressivement être remplacés par des outils rédactionnels artificiels ? Les présentateurs pourraient-ils être supplantés par des avatars virtuels ? Des expérimentations concrètes en ce sens ont déjà été menées à travers le monde. Des projets comme Channel 1 aux États-Unis ont annoncé vouloir créer des chaînes d'information présentées par des avatars virtuels générés par IA, tandis que des initiatives comme NewsGPT ou le podcast Daily News de Perplexity proposent la production automatisée de contenus textes ou audios.

Au-delà des effets d'annonce, la présence d'avatars ne signifie pas systématiquement la disparition totale du contrôle humain puisque

des journalistes ou éditeurs peuvent continuer de superviser, valider ou écrire les contenus en amont. En outre les projets de médias entièrement automatisés restent largement expérimentaux ou inaboutis : Channel 1, par exemple, a depuis abandonné l'idée d'une chaîne 100 % IA pour se recentrer sur des outils d'adaptation et de personnalisation de contenus, montrant que les ambitions initiales autour de l'automatisation complète ont été revues à la baisse.

Néanmoins ces expérimentations démontrent qu'il est indispensable que les médias publics et privés s'emparent de l'intelligence artificielle, réfléchissent à la manière de garder la maîtrise sur leurs pratiques, leur indépendance



« En déléguant certaines opérations répétitives à l'IA, nous libérons de l'espace pour ce qui fait la véritable richesse du métier. »

éditoriale et accompagnent le développement de l'intelligence artificielle générative de manière responsable.

La RTBF, depuis plus de deux ans, a pris le dossier en main, non sans interrogations ou inquiétudes au sein de sa rédaction et plus largement de l'entreprise. Ces interrogations traduisent aussi une volonté d'agir avec discernement et anticipation. En effet, dans nos métiers encadrés par la loi, la déontologie, pour lesquels la rencontre, l'humain, la protection des sources, la vérification et la rigueur sont fondamentaux, comment pouvons-nous intégrer des outils d'intelligence artificielle ? Comment pouvons-nous continuer à assurer notre fiabilité en montant à bord du train de cette révolution ?

Pour structurer sa démarche, la RTBF s'est dotée d'une gouvernance de l'IA et des algorithmes, articulant innovation et éthique éditoriale, mobilisant des équipes pluridisciplinaires réunissant des expertises technologiques, datas, éditoriales, de production ou juridiques. Notre média de service public s'est notamment concerté avec les Médias Francophones Publics (MFP) et a adopté ses propres balises afin d'encadrer l'usage de l'IA en son sein :

- Toute génération de contenu à l'aide d'une IA doit se faire dans un cadre éditorial supervisé par l'humain.
- Il est interdit de répliquer l'image ou la voix de personnes existantes à l'aide d'une IA, sauf dans le cadre d'expérimentations clairement identifiées comme telles.
- Aucune donnée confidentielle ne peut être transmise à une IA.
- Tout contenu significativement généré par une IA doit être identifié comme tel.

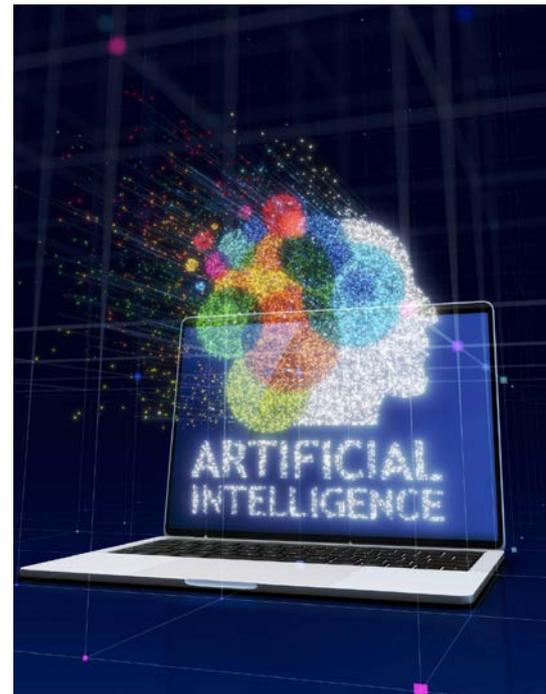
Ces balises RTBF peuvent être révisées en fonction de l'évolution des outils technologiques et des usages.

Concrètement, les journalistes de la RTBF peuvent ainsi utiliser l'IA dans plusieurs cas de figure. Elle est particulièrement utile pour automatiser des tâches à faible valeur ajoutée, comme la retranscription d'interviews, le traitement initial des textes ou de données. Elle permet aux journalistes de gagner du temps et de se concentrer sur des activités à forte valeur journalistique : mettre en perspective les propos recueillis, donner du sens aux informations, recouper les faits avec rigueur et éclairer le public avec une analyse approfondie. En déléguant certaines opérations répétitives à l'IA, nous libérons de l'espace pour ce qui fait la véritable richesse du métier. La supervision humaine journalistique est indispensable, de même que le choix de ne pas utiliser l'outil d'IA, par exemple pour des interviews confidentielles ou des sources à protéger et dont il ne faut pas laisser de traces digitales.

Lors des dernières élections communales, à l'automne 2024, grâce à l'IA, notre rédaction a testé pour la première fois l'assistance à la génération d'articles factuels afin de rendre compte des résultats des élections dans toutes les communes. Ces articles contenaient des chiffres bruts sans aucune interprétation ; ils nous ont permis d'assurer notre mission d'information à destination de l'ensemble de la population des communes belges francophones. La génération de ces articles a également permis aux journalistes des rédactions locales de se délester de tâches basiques et de se concentrer sur du reportage de terrain, des interviews, des analyses ou de la mise en perspective. La génération d'articles a été effectuée sous

supervision éditoriale et journalistique en chair et en os.

Lors des JO de Paris la rédaction sportive a utilisé l'IA générative pour faciliter la rédaction des articles qui présentaient les règles de chaque épreuve olympique, un contenu fastidieux à rédiger et sans plus-value journalistique majeure. Le temps libéré a pu être consacré à des contenus centrés sur les performances attendues par le camp belge dans chacune de ces disciplines. L'IA a aussi été mise à contribution lors de la Coupe du monde féminine de football. Un outil de résumé automatique des matches a permis de couvrir en vidéo l'ensemble de la compétition sur les plateformes numériques de la RTBF.





« Nous entrons dans une dynamique de contenus dits “liquides”, où les contenus ne sont plus présentés sous leur forme éditoriale originale, mais sont fragmentés, recombinaés et adaptés en temps réel au contexte et aux besoins spécifiques de chaque utilisateur. »



Plusieurs utilisations de l'IA ont été testées au cours des dernières années dans notre rédaction comme dans d'autres. Une étude commandée par la Commission paritaire nationale emploi et formation (CPNEF) de l'audiovisuel en France (<https://www.afdas.com/actualites/communiquede-presse/lia-generative-dans-le-journalisme-audiovisuel-queles-usages-et-queles-transformations-pour-les-professionnels.html>) a identifié de nombreuses possibilités sur l'ensemble de la chaîne de production des médias : la veille sur les informations et la détection de tendances ; la recherche et l'analyse de données ; la facilitation de la production concernant le montage, la transcription, la traduction ou la génération d'images ; l'adaptation de contenus pour différents canaux de diffusion. La validation éditoriale – en fin de chaîne de production – reste la prérogative de l'humain à la RTBF.

Mais jusqu'où aller ? Que pouvons-nous accepter et que devons-nous refuser ? Ces réflexions ouvrent un débat sur l'éthique et l'innovation dans le journalisme. Chaque média se fixe ses limites et les réinterroge au fur et à mesure du développement fulgurant des outils d'IA.

Beaucoup de tests sont en cours dans notre rédaction RTBF comme dans de nombreux médias d'information à travers le monde, mais au-delà des promesses annoncées ou des gains théoriques, l'usage montre la nécessité d'investir du temps et de l'argent pour analyser des outils, les tester, les rendre fiables puis soutenir leur implémentation dans une rédaction. Les rédactions doivent également abandonner des projets qui pourraient porter atteinte à leur crédibilité, et chacune d'entre elles fait le choix d'outils d'intelligence artificielle en fonction de sa ligne éditoriale, de son éthique ou de sa culture.

Ainsi, pour la première fois en France, dans le documentaire « Nous, jeunesse(s) d'Iran » (France TV), la réalisatrice Solène Chalvon-Fioriti a donné la parole à des jeunes Iraniens en anonymisant et en transformant leur visage au moyen de l'intelligence artificielle, tout en conservant leur expression faciale ; une manière de préserver une certaine expressivité et une forme de réalisme émotionnel, tout en protégeant leur anonymat dans un pays où celles-ci risquent leur vie. Le recours à l'IA est signalé de manière transparente, certes, mais il peut aussi questionner : dans quelle mesure cela pourrait affecter la confiance du public dans la véracité du propos ?

La question mérite d'être posée alors même que la confiance du public à l'égard du travail des médias constitue un enjeu majeur. Une étude de l'Université du Kansas (<https://news.ku.edu/news/article/study-finds-readers-trust-news-less-when-ai-is-involved-even-when-they-dont-understand-to-what-extent>) publiée en novembre 2024 a ainsi montré que lorsque les lecteurs pensent que l'intelligence artificielle est impliquée d'une manière ou d'une autre dans la production des informations, ils ont moins confiance dans la crédibilité des informations.

Ce manque de confiance ne serait pas infondé. C'est ce que tend à démontrer une étude de la BBC publiée en février 2025 (<https://www.bbc.com/mediacentre/2025/bbc-research-shows-issues-with-answers-from-artificial-intelligence-assistants>) et réalisée durant un mois sur quatre outils d'IA. Elle révèle de nombreuses erreurs générées par l'utilisation d'assistants d'intelligence artificielle pour répondre à des questions sur l'actualité : plus de la moitié des réponses de l'IA « ont été jugées comme présentant des problèmes importants sous une forme ou une autre » et près de 20 %

Profession

des réponses de l'IA « qui citent le contenu de la BBC présentait des erreurs factuelles ».

À ceci s'ajoutent les interrogations sur la propriété intellectuelle des données et productions d'informations des médias reprises par les intelligences artificielles dans un flou algorithmique important.

Il est donc essentiel d'aborder l'évolution de l'intelligence artificielle avec lucidité, en reconnaissant ses limites mais sans freiner les dynamiques de transformation déjà à l'œuvre dans nos rédactions. Les évolutions technologiques touchent progressivement l'ensemble des métiers des médias, comme le résume l'étude de la CPNEF : « [L]es journalistes desk, les documentalistes, motion designers, monteurs ou réalisateurs ; des métiers dits augmentés par l'automatisation de certaines de leurs activités, comme les reporters, rédacteurs en chef, datajournalistes ou fact-checkeurs ; des traducteurs et interprètes [...] ou présentateurs et animateurs d'antenne ». Il nous revient d'accompagner ces changements afin d'enrichir nos pratiques, ouvrir de nouvelles perspectives, renforcer la qualité de l'information, mieux répondre aux attentes du public et à l'évolution de sa consommation de l'information.

Ainsi le déploiement d'un outil comme Google AI Overviews (bientôt disponible en Belgique) via lequel Google propose à l'internaute une réponse synthétique à sa question sans qu'il ait eu besoin de consulter des liens des contenus qui ont nourri la synthèse, ou l'habitude de plus en plus répandue, en particulier dans les nouvelles générations, d'interroger, non plus un moteur de recherche comme Google, mais



directement un chatbot comme ChatGPT ou Perplexity, annoncent une nouvelle vague de désintermédiation de l'accès à l'information, c'est-à-dire de réduction ou suppression des intermédiaires entre le média producteur d'information et le public.

Nous entrons dans une dynamique de contenus dits « liquides », où les contenus ne sont plus présentés sous leur forme éditoriale originale, mais sont fragmentés, recombinaison et adaptés en temps réel au contexte et aux besoins spécifiques de chaque utilisateur. Cette évolution, qu'on le veuille ou non, redéfinit la manière dont l'information est découverte, consommée et perçue. Elle ouvre un débat fondamental sur le rôle que doivent jouer les médias d'information dans un monde où les moteurs de réponse et les intelligences artificielles structurent l'accès aux contenus.

L'intelligence artificielle, comme tout nouvel outil, représente donc des risques et des opportunités pour notre rédaction RTBF comme pour tous les médias. Il nous revient d'explorer les possibilités de faciliter ou automatiser des tâches à divers niveaux de la chaîne de valeur des rédactions, tout en conservant la maîtrise de l'analyse et de la décision éditoriale. L'IA offre également la possibilité de se recentrer sur l'essentiel : l'humain et la valeur démocratique du journalisme. Retrouver du temps pour aller sur le terrain et rencontrer la population, développer l'information de proximité et d'intérêt public, mener des enquêtes approfondies et du *fact-checking*, accroître la transparence sur notre métier et la manière de le pratiquer, voilà autant de domaines que les médias peuvent encore développer pour se différencier des outils d'intelligence artificielle.

Les révolutions technologiques ont toutes suscité inquiétudes et enthousiasme, elles ont profondément transformé des métiers, en ont supprimé beaucoup et créé d'autres. Elles ont touché les paysans et les ouvriers ; aujourd'hui, elles concernent les cols blancs et les tâches intellectuelles. En tant que média, nous pouvons intégrer l'intelligence artificielle pour autant qu'elle améliore notre travail, tout en veillant à garder le contrôle humain. C'est à nous de trouver l'équilibre entre les deux. Il en va de la survie de notre métier et de la confiance du public.





Axel
Beelen

Juriste spécialisé en
donnée et en IA

—
[https://www.
axelbeelen.be](https://www.axelbeelen.be)

—
X @beelbax



Jeffrey
Vigneron

Avocat et fondateur
du cabinet Lawgitech

—
<https://lawgitech.eu/>



CYBERSÉCURITÉ : UN IMPÉRATIF ÉGALEMENT POUR LES CABINETS D'AVOCAT(E)S

Cybersicherheit: auch für Anwaltskanzleien ein Muss!

Anwaltskanzleien, die Hüter von sensiblen Informationen sind, sind zu beliebten Zielen für Cyberkriminelle geworden. Von Ransomware, die den Betrieb lahmlegt und Geld erpresst, über den Diebstahl vertraulicher Daten, der ganze Akten gefährden kann, bis hin zu Denial-of-Service-Angriffen, die den Zugang zu Online-Diensten blockieren, bleibt keine Struktur verschont – egal ob es sich um eine kleine Sozietät oder eine große internationale Kanzlei handelt. Die Zunahme von Cyberangriffen und das Inkrafttreten der NIS-2-Richtlinie (die in belgisches Recht umgesetzt wurde) zwingen Anwaltskanzleien, ihre digitale Sicherheit zu verbessern. Lassen Sie uns in den folgenden Zeilen ergründen, warum und wie.

Les cabinets d'avocats, dépositaires de secrets sensibles, sont devenus des cibles de choix pour les cybercriminels. Des rançongiciels paralysant

l'activité et extorquant des fonds, aux vols de données confidentielles pouvant compromettre des dossiers entiers, en passant par des attaques par déni de service qui bloquent l'accès aux services en ligne, aucune structure n'est épargnée – qu'il s'agisse d'un petit cabinet ou d'une

grande firme internationale. La multiplication de ces cyberattaques et l'entrée en vigueur de la directive NIS 2 (transposée en droit belge) imposent dorénavant aux cabinets d'avocats de renforcer leur sécurité numérique. Voyons pourquoi et comment dans les lignes qui suivent.



« En cas de manquement grave à la sécurité conduisant à la divulgation de secrets de clients, un avocat pourrait non seulement subir une sanction disciplinaire, mais aussi engager la responsabilité civile du cabinet. »

Des cabinets d'avocat(e)s sous la menace des cyberattaques

Les cabinets d'avocats cumulent plusieurs facteurs de risque en matière de cybersécurité. En effet, leurs systèmes informatiques renferment souvent des données confidentielles (données personnelles de clients, pièces de procédures, stratégies juridiques, secrets d'affaires) qui ont une grande valeur. Les rançongiciels exploitent cette valeur : les acteurs malveillants savent qu'un cabinet touché fera tout pour éviter la divulgation de ses dossiers. *En 2024, les attaques par rançongiciel ont particulièrement touché les entreprises de services professionnels, catégorie dans laquelle figurent les cabinets d'avocats.* Par ailleurs, les vecteurs d'intrusion les plus courants – phishing (hameçonnage par courriel), pièces jointes piégées, vulnérabilités non corrigées – trouvent souvent une cible facile dans des structures où la sécurité n'est pas encore prioritaire. Une simple campagne de courriels frauduleux bien conçue peut tromper un collaborateur et ouvrir la porte du réseau du cabinet. Nul n'est à l'abri malheureusement...

Les cabinets d'avocat(e)s, gardiens de données sensibles, désormais sur la ligne de front des cybermenaces

Les conséquences d'une cyberattaque pour un cabinet sont multiples : interruption d'activité en cas de système bloqué, violation du secret professionnel si des données client sont consultées, atteinte à la réputation du cabinet, sans parler des coûts de restauration des systèmes et des éventuelles suites juridiques. À titre d'exemple, une attaque de type rançongiciel chiffrant l'ensemble des dossiers numériques, pourrait paralyser le cabinet pendant des jours, tandis qu'une fuite de données pourrait exposer publiquement des informations confidentielles

sur des clients, engageant la responsabilité du cabinet. Dans un tel contexte, la question n'est plus de savoir si une cyberattaque surviendra, mais quand.

Obligations légales et déontologiques : RGPD et secret professionnel

Au-delà du simple bon sens, les avocats ont déjà des obligations minimales en matière de cybersécurité découlant de la réglementation et de la déontologie. En effet, depuis le 25 mai 2018, le Règlement général sur la protection des données (RGPD) impose, à son article 32, aux responsables de traitement – ce qui inclut les cabinets d'avocats traitant des données personnelles de clients – de mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données personnelles. Cela implique notamment

d'assurer la confidentialité, l'intégrité et la disponibilité des données traitées. Concrètement, un cabinet doit, par exemple, chiffrer les données sensibles lorsqu'il le peut, utiliser des moyens d'authentification robustes, protéger ses réseaux informatiques, sauvegarder régulièrement ses fichiers et tester l'efficacité de ces mesures.

Par ailleurs, le secret professionnel des avocats – socle de la relation de confiance avec le client – impose une confidentialité absolue des informations confiées. Cette obligation déontologique implique, à l'ère du numérique, de sécuriser les communications électroniques (chiffrement des e-mails ou utilisation de messageries sécurisées), de protéger l'accès aux dossiers numérisés et de veiller à ce que seuls les membres autorisés de l'équipe puissent consulter les informations couvertes par le



secret. En cas de manquement grave à la sécurité conduisant à la divulgation de secrets de clients, un avocat pourrait non seulement subir une sanction disciplinaire, mais aussi engager la responsabilité civile du cabinet. Autrement dit, depuis longtemps, la cybersécurité fait partie pleinement du devoir de confidentialité de l'avocat.

Directive NIS 2 : le nouveau cadre européen de la cybersécurité

Entrée en vigueur fin 2022, la directive européenne NIS 2 (Directive (UE) 2022/2555) marque un tournant dans la régulation de la cybersécurité au sein de l'UE. Son objectif est d'assurer un niveau élevé et harmonisé de cybersécurité pour les services essentiels et autres services critiques au bon fonctionnement de nos sociétés. Contrairement à la première directive NIS, qui laissait une marge de manœuvre aux États membres de l'UE, NIS 2 impose des règles communes plus strictes en matière de gestion des risques et de notification des incidents.

NIS 2 s'applique à un large éventail de secteurs jugés critiques. Son champ d'application a été étendu par rapport à la précédente directive : elle couvre désormais, entre autres, les services publics, certaines industries manufacturières, la recherche, la gestion des déchets, ou encore les infrastructures numériques, en plus des secteurs déjà couverts comme l'énergie, les transports, la finance, la santé, l'eau. Les entités visées sont classées en deux catégories : les entités essentielles (secteurs hautement critiques de l'Annexe I de la directive, par ex. un opérateur d'énergie ou un grand hôpital) et les entités importantes (autres secteurs critiques de l'Annexe II, par ex. un fournisseur alimentaire majeur ou un service postal). La différence tient principalement au régime de supervision et de sanctions, plus strict évidemment pour les entités essentielles.

Pour toutes ces entités, NIS 2 impose un ensemble d'obligations minimales de cybersécurité. Chaque organisation concernée doit en effet évaluer ses risques et mettre en place des mesures de sécurité appropriées et proportionnées (gouvernance de la sécurité, protection des réseaux et systèmes, gestion des identités, etc.). Elle doit également notifier aux autorités compétentes toute violation de sécurité significative dans des délais serrés (sous 24 heures pour un premier signalement, selon la loi belge de transposition – un délai fortement plus court que celui du RGPD). La responsabilité du conseil d'administration ou des dirigeants peut être explicitement engagée en cas de manquement à ces obligations, ce point soulignant à suffisance que la cybersécurité n'est plus uniquement une affaire de technicien mais bien un enjeu de gouvernance des entreprises et des institutions publiques. En Belgique, la directive a été transposée par la loi du 26 avril 2024 relative à la cybersécurité des réseaux et systèmes d'information d'intérêt général pour la sécurité publique, complétée par l'arrêté royal du 9 juin 2024. Le Centre pour la Cybersécurité Belgique (le CCB) y a été désigné comme autorité de coordination et de contrôle du nouveau cadre.

Les cabinets d'avocats ne figurent pas directement parmi les entités visées par NIS 2, les services juridiques n'étant pas listés en tant que secteur critique au sens de la directive. Cependant, la directive va tout de même concerner la profession de manière indirecte, via ses effets en cascade.

Effet domino : la sécurité de la chaîne d'approvisionnement

NIS 2 innove en effet en exigeant des entités essentielles et importantes qu'elles renforcent la sécurité de leur chaîne d'approvisionnement. En d'autres termes, une entreprise soumise à

NIS 2 doit s'assurer que ses fournisseurs et prestataires de services critiques appliquent eux aussi des normes de cybersécurité adéquates. La directive prévoit que les politiques de sécurité mises en place couvrent les relations avec les tiers (fournisseurs IT, sous-traitants, etc.), afin de prévenir le risque qu'un attaquant passe par un maillon faible pour atteindre l'entité principale.

Or, beaucoup de cabinets d'avocats fournissent des services juridiques à des clients qui, eux, entrent dans le champ de NIS 2. On peut citer les cabinets conseillant des opérateurs d'énergie, des banques, des hôpitaux ou des organismes publics – tous classés entités essentielles – ou encore ceux travaillant pour des entreprises de secteurs « Annexe II » (transport, industrie, etc.). Dans ce contexte, les cabinets en question deviennent une extension de la surface de risque de leurs clients. *Un cabinet d'avocats mal sécurisé peut constituer la porte d'entrée d'une attaque envers une entité essentielle.* En effet, des hackers pourraient cibler le cabinet X pour voler des documents sensibles liés à un projet d'infrastructure énergétique, ou pour usurper l'identité du conseil juridique et envoyer de faux courriels piégés au sein de l'entreprise cliente.

Les clients soumis à NIS 2 demanderont donc dorénavant des garanties de sécurité renforcées de la part de leurs conseils juridiques. Ils exigeront d'avoir, dans vos lettres de mission, des clauses contractuelles de cybersécurité. Ces clauses devront détailler vos mesures de sécurité informatique, quelles seront vos actions en cas d'incident constaté dans votre cabinet, etc. Vos clients pourraient aussi vous envoyer des questionnaires d'audit ou vous demander de réaliser des évaluations régulières de votre sécurité informatique. Il se pourrait aussi qu'ils exigent de votre part d'avoir des certifications en la matière (ISO 27001 par exemple).

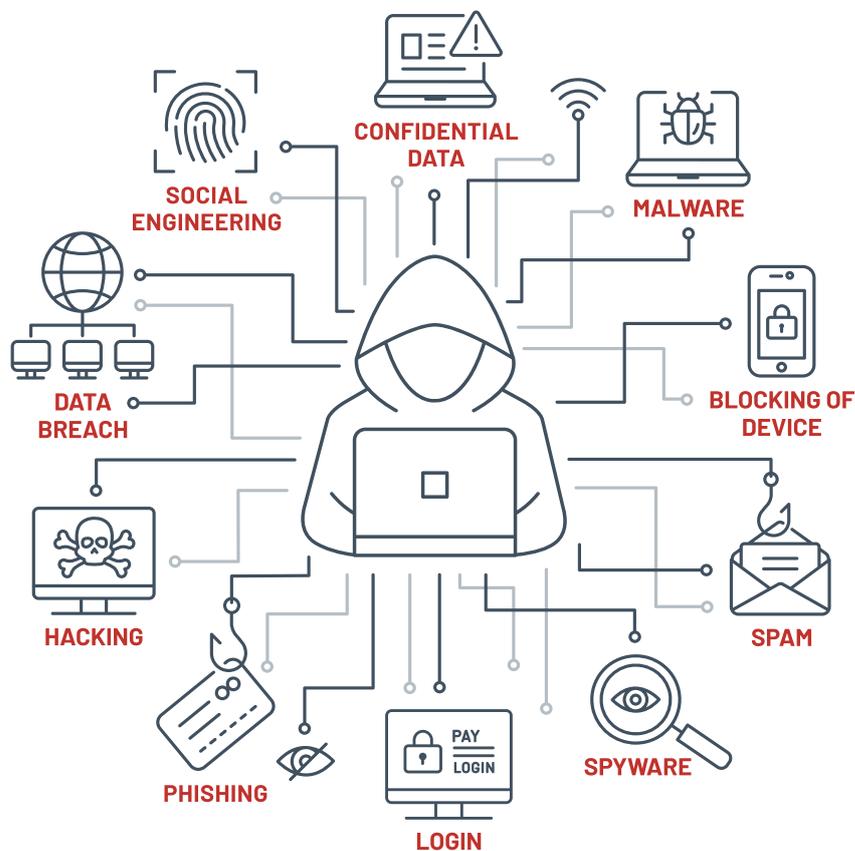
Nous assistons à un véritable changement de paradigme. En effet, là où, historiquement, la sécurité des informations échangées reposait souvent uniquement sur la confiance dans le secret professionnel, *les clients des cabinets d'avocats exigent de plus en plus que lesdits cabinets aient implémenté une réelle démarche formalisée de due diligence numérique.*

En d'autres mots, même sans être directement visés par NIS 2, les avocats vont en ressentir son influence à travers les exigences de leurs clients. Les cabinets d'avocats qui anticiperont ces attentes en se conformant volontairement et de manière anticipée à des normes de cybersécurité robustes bénéficieront d'un véritable avantage concurrentiel, tandis que les cabinets négligeant la sécurité risquent de se voir écartés de certains marchés ou dossiers sensibles. Vous l'avez compris, la cybersécurité est devenue un critère de qualité, de fiabilité et de différenciation dans la chaîne de prestation des services juridiques.

Notre conseil : renforcer maintenant la cyber-résilience de votre cabinet

Face à ces constats, tout cabinet d'avocats a intérêt à adopter une stratégie proactive pour améliorer sa cyber-résilience. Voici quelques mesures pratiques et recommandations pour protéger votre structure et rassurer vos clients :

- Adoptez un référentiel de sécurité reconnu : un bon point de départ est de suivre le référentiel CyberFundamentals (ou CyFun) du CCB. Ce cadre propose un ensemble de mesures concrètes pour protéger les données et réduire significativement les risques liés aux attaques les plus courantes. Il est possible de faire certifier son organisation selon plusieurs niveaux (Basic, Important, Essentiel) en fonction du niveau de menace à couvrir. En obtenant le label CyFun, votre cabinet démontrera qu'il respecte une norme reconnue de bonnes pratiques en cybersécurité et qu'il a ainsi mis en place de contrôles essentiels pour sécuriser ses systèmes et données (personnelles et non personnelles).



- Assurez une hygiène numérique irréprochable à l'ensemble de vos collaborateurs : la majorité des incidents provient de failles basiques facilement évitables. C'est pourquoi, il est essentiel de mettre à jour régulièrement vos logiciels et systèmes informatiques, d'utiliser un antivirus/anti-malware à jour lui aussi sur tous les postes, et d'effectuer des sauvegardes fréquentes de vos dossiers (avec copies hors-ligne) afin de pouvoir restaurer vos données en cas d'attaque. Segmentez votre réseau interne pour éviter qu'une intrusion ne se propage à l'ensemble du cabinet. Ces mesures de cyber-hygiène de base forment la première ligne de défense et réduisent considérablement les risques courants (rançongiciel, virus, intrusion automatisée).
- Renforcez l'authentification et le contrôle d'accès : protégez l'accès à vos systèmes et données par des mécanismes robustes et reconnus. Nous vous conseillons fortement d'activer dès aujourd'hui l'authentification multi-facteur (MFA) sur vos boîtes e-mail et sur tout service sensible. L'authentification multi-facteur ajoute une couche de sécurité en

demandant, par exemple, un code sur mobile en plus du mot de passe. Mettez aussi en place des politiques de mots de passe solides. Limitez les droits d'accès selon le principe du moindre privilège : chaque utilisateur ne doit accéder qu'aux dossiers et applications nécessaires à ses activités. Revoyez aussi annuellement ces politiques d'accès. Pensez à verrouiller les postes et appareils mobiles par des codes ou empreintes, et à chiffrer les disques durs des ordinateurs portables. En cas de départ d'un collaborateur, assurez-vous de désactiver immédiatement ses différents accès.

- Formez et sensibilisez votre équipe : la technologie ne peut pas tout, le facteur humain reste déterminant. Organisez des formations internes courtes sur les bonnes pratiques de sécurité (celles-ci évoluant avec le temps, ces formations devront être reproduites avec le temps). Apprenez à vos équipes comment reconnaître un e-mail de phishing, quels réflexes ils doivent adopter en cas de doute, l'importance de ne pas brancher de clé USB inconnue, etc. Vous

pouvez simuler périodiquement des tests d'hameçonnage (envoi de faux e-mails) pour évaluer et améliorer la vigilance de tous. Affichez quelques règles simples au bureau (par exemple, procédures pour le transfert d'argent ou la vérification d'instructions par téléphone, afin d'éviter les arnaques au président ou au faux notaire où les personnes mal intentionnées se font passer par des dirigeants pressés pour demander des transferts urgents d'argent). Avoir une culture de cybersécurité au sein du cabinet est l'un des meilleurs remparts contre les attaques sociales. C'est véritablement chaque membre du personnel – associé, juriste, paralégal, secrétaire – qui doit se sentir concerné et qui

doit être un des acteurs de la protection du cabinet (et des informations de ses clients).

- Anticipez les incidents : enfin, préparez-vous au scénario du pire pour réagir efficacement. Vous devez établir dès à présent un plan de réponse aux incidents. Ce plan doit décrire qui contacter (police fédérale, expert IT, assurance cyber, clients...) en cas de cyberattaque, comment isoler les systèmes touchés, comment communiquer en interne et en externe, etc. Ce plan/politique interne doit être

connu(e) de chacun des membres de votre personnel et revu(e) régulièrement. L'important, vous l'avez compris, est, dès à présent, de ne pas être pris au dépourvu lorsque l'incident se produira. En effet, dans le cas où votre cabinet est bien préparé, il saura contenir l'attaque et pourra redémarrer plus vite, limitant les dégâts juridiques et réputationnels (et ces derniers peuvent être très importants et très difficiles à recouvrir).

Notre conseil

La cybersécurité doit devenir une composante à part entière de la gestion de votre cabinet d'avocats, au même titre que le suivi des autres évolutions légales ou de sa gestion financière. La directive NIS 2 énonce que la résilience numérique de l'ensemble de la chaîne de services (juridiques mais pas que) est désormais primordiale. Pour les avocats, c'est à la fois un défi et une opportunité : celui de faire évoluer leurs pratiques et leurs différents outils vers plus de sécurité, et de pouvoir le valoriser auprès de leurs clients. Nous vous conseillons d'adopter dès aujourd'hui les bonnes pratiques de cybersécurité. Vous protégerez ainsi votre cabinet et vos clients, mais vous vous conformerez aussi aux attentes croissantes d'un marché toujours plus concurrentiel et à celles du régulateur.



Johannes
Seel

Avocat
Médiateur agréé
Ombudsman local
d'Avocats.be

<https://www.linkedin.com/in/johannes-seel>

j.seel@avocat.be



L'ATTITUDE DU CLIENT ET DE LA CLIENTE FINAL(E) FACE AUX NOUVELLES TECHNOLOGIES : LEÇONS TIRÉES D'UNE ÉTUDE BELGE

Die *Einstellung* des Mandanten zu *neuen Technologien*: Erkenntnisse aus einer belgischen Studie

Im September 2022 führten Wissenschaftler der Universität Antwerpen in Zusammenarbeit mit dem der VOG Conflicool eine umfassende empirische Studie über den Vertrauensgrad der belgischen Öffentlichkeit mit alternativen Methoden der Streitbeilegung durch. Ein repräsentativer Querschnitt der nationalen Bevölkerung – 2005 Bürger Belgiens – nahm an der von YouGov durchgeführten Umfrage teil.

Die Umfrage befasste sich auch mit dem Einsatz digitaler Technologien bei der Streitbeilegung, die auch unter dem Akronym ODR (Online Dispute Resolution) bekannt sind. Dieser Artikel konzentriert sich ausschließlich auf die Ergebnisse im Zusammenhang mit diesen Technologien.

Sources d'information en cas de litige

Lorsque les répondants ont été interrogés sur leur *premier* réflexe en cas de conflit, 28 % ont déclaré se tourner vers l'Internet.

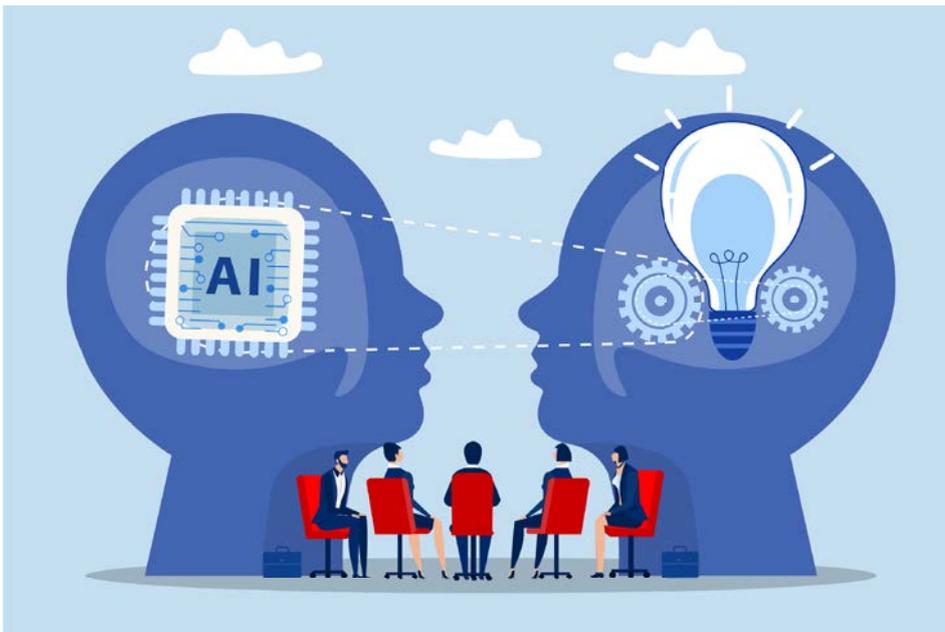
Parmi les personnes qui ont effectivement eu un conflit perçu comme grave au cours des trois dernières années, 45 % ont *également* utilisé des sites Internet pour obtenir des

informations sur les possibilités de règlement des litiges.

Le web constitue donc une source d'information essentielle pour une part importante de la population.

En septembre 2022, des chercheurs de l'Université d'Anvers, en collaboration avec l'ASBL Conflicool, ont conduit une vaste étude empirique sur le degré de familiarité du public belge avec les méthodes alternatives de résolution des différends. Un échantillon représentatif de la population nationale – 2005 citoyens belges – a répondu au sondage administré par YouGov. L'enquête s'est également intéressée à l'utilisation des technologies numériques dans la résolution des conflits, également connues sous l'acronyme ODR (Online Dispute Resolution). Cet article se concentre exclusivement sur les résultats liés à ces technologies.

Profession



Confiance dans les solutions technologiques

Il a également été demandé aux participants s'ils se sentent à l'aise avec les nouvelles technologies. Les réponses sont nuancées :

- 48 % des personnes interrogées ont adopté une position neutre ;
- 25 % se sont dit à l'aise (plutôt ou très à l'aise) ;
- 27 % ont exprimé un malaise (peu ou pas du tout à l'aise).

Pour accroître leur confiance envers ces outils numériques, les participants ont cité plusieurs facteurs clés :

- 50 % souhaiteraient disposer de plus d'informations sur les ODR ;
- 33 % veulent s'assurer que les décisions obtenues soient équitables ;
- 29 % indiquent qu'une familiarité préalable avec ces outils, ou une expérience directe, renforcerait leur confiance.

La transparence apparaît donc comme un élément central pour favoriser l'acceptation de ces technologies.

Perception de l'efficacité des ODR

Lorsque l'on interroge les répondants sur les fonctionnalités technologiques qui leur

semblent les plus utiles pour résoudre les conflits :

- 39 % mettent en avant les outils qui soutiennent les parties (modèles, guides, etc.) ;
- 36 % apprécient les outils de gestion administrative (planification de rendez-vous, organisation logistique...);
- 29 % sont intéressés par des systèmes d'analyse prédictive de l'issue juridique d'un différend ;
- Seulement 6 % voient favorablement une décision rendue directement par une intelligence artificielle.

En résumé, si les citoyens belges perçoivent clairement les avantages de certains outils numériques pour faciliter le règlement des litiges – notamment ceux favorisant l'information et l'organisation –, ils demeurent réticents à confier l'issue de leurs conflits à des algorithmes.

Conclusion

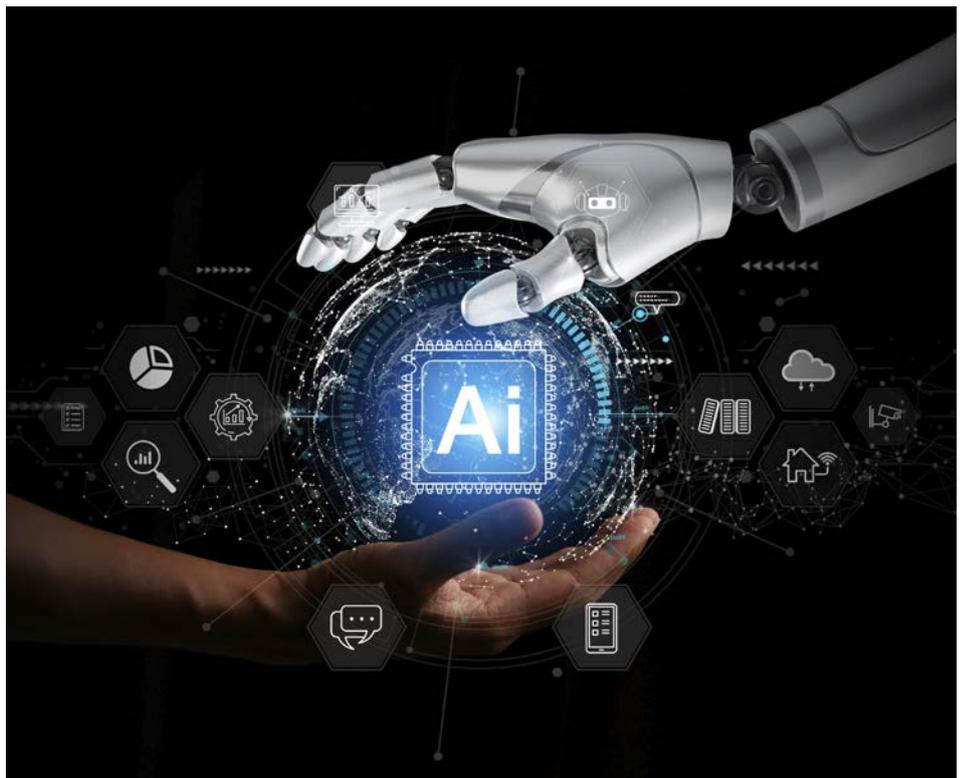
Pour notre part, les nouvelles technologies ne sont ni bonnes ni mauvaises. Ce qui compte, c'est de garantir que leur utilisation profite principalement aux utilisateurs finaux.

La méfiance exprimée par certains répondants à l'égard des décisions rendues par l'intelligence artificielle souligne aussi que l'humain reste central dans le règlement des litiges : les avocats conservent un rôle clé de conseiller, défenseur et d'interprète du droit.

Bibliographie

Plateforme – Les statistiques d'utilisation de la plateforme conflicool (www.conflicool.org) peuvent être mises à disposition sur demande (contact avec l'auteur via <https://www.linkedin.com/in/johannes-seel>)

Sondage – Rutten, S. (2022). Baromètre de la résolution des litiges en Belgique : attitudes et expériences des citoyens en matière de gestion des problèmes juridiques. Résultats d'une enquête à grande échelle menée auprès de la population belge par l'Université d'Anvers, YouGov et Conflicool. L'équipe de recherche : Rutten, S., Vanlerberghe, B., Nigmatullina, D., Beretta, R., & Seel, J. Les résultats sont accessibles via le lien suivant : <https://conflicool.org/fr-be/survey>.



Notre conseil

Un enjeu stratégique pour les avocat(e)s

À la lumière des résultats du sondage, un conseil s'impose aux avocats : anticiper l'évolution des attentes de leurs clients en matière de résolution de litiges. Cela passe par une meilleure connaissance des outils ODR, une intégration réfléchie des technologies dans leur pratique quotidienne, et surtout, une capacité à expliquer et encadrer leur utilisation. Les avocats qui sauront combiner expertise juridique, communication claire et ouverture aux innovations numériques renforceront leur positionnement dans un paysage en mutation. La confiance se construit aujourd'hui autant sur la maîtrise du droit que sur la capacité à naviguer dans un environnement digital.





Jean-François
Henrotte

Avocat

<http://www.lexing.be>

[@Henrotte](#)



LA JUSTICE DU SENS : L'IA AU SERVICE DE LA TRADUCTION

KI im Dienste der Übersetzung

Wie wir alle wissen, geht es beim Übersetzen nicht darum, Wörter zu übertragen, sondern eine Bedeutung wiederzugeben. Eine gute Übersetzung ist also mehr als nur eine wörtliche Übersetzung, sondern eine echte Kommunikationsübung, bei der Treue, Präzision und kulturelle Korrektheit von entscheidender Bedeutung sind.

Von den ersten Versionen, die Systran anbot, oder den Anfängen von Google Translate sind wir heute weit entfernt. Dank der Fortschritte in der künstlichen Intelligenz werden maschinelle Übersetzungen immer präziser: Sie entfernen sich vom Wörtlichen und nähern sich manchmal sogar dem Literarischen.

Und als Sahnehäubchen auf dem belgischen Kuchen werden auch die Übersetzungen ins Niederländische immer überzeugender.

In diesem Artikel haben wir uns dafür entschieden, nicht niederländische, sondern englische Übersetzungen zu vergleichen.

Chacun le sait : traduire, ce n'est pas transposer des mots, mais restituer un sens. Une bonne traduction ne se limite donc pas à une conversion littérale ; elle constitue un véritable exercice de communication, où fidélité, précision et justesse culturelle sont essentielles.

Nous sommes aujourd'hui bien loin des premières versions proposées par Systran ou les débuts de Google Translate. Grâce aux avancées en intelligence artificielle, les traductions automatiques gagnent en finesse : elles s'éloignent du littéral pour se rapprocher, parfois, du littéraire.

Et, cerise sur le gâteau belge, les traductions en néerlandais deviennent elles aussi de plus en plus convaincantes.

Dans cet article, nous avons pourtant choisi de comparer des traductions non pas en néerlandais, mais en anglais. Parce que la maîtrise de l'anglais reste largement répandue chez nos lecteurs. Par ailleurs, nous n'avons pas voulu choisir la meilleure traduction. Plutôt que de désigner un « meilleur » outil,

notre objectif est ici de vous montrer l'état actuel des performances en matière de traduction juridique automatisée. Car oui, ces outils sont aujourd'hui efficaces, à condition de rester supervisés par un juriste compétent.

Nous vous invitons donc à parcourir les différentes versions traduites d'une lettre de mise en demeure simple, pour juger par vous-même. Bonne lecture !

Profession

Original en français

MISE EN DEMEURE

PAR RECOMMANDÉ AVEC ACCUSÉ DE RÉCEPTION

Bruxelles, le 27 mai 2015

Votre réf. : _____

Notre réf. : _____ – _____

Chère Madame,

La présente vous est adressée en notre qualité de conseil de la SA SOCIÉTÉ Y, dont le siège social est établi à _____, inscrite à la BCE sous le numéro _____ – Tél. : _____ – e-mail : _____.

Vous êtes redevable envers notre cliente de la somme en principal de _____ € en raison de factures impayées, établies entre les mois de mai 2023 et d'avril 2025, en exécution d'un contrat de fourniture de mazout.

Du fait de votre absence de paiement dans les délais contractuels, votre dette s'élève désormais à la somme de _____ € conformément au décompte suivant :

- en principal : _____ €
- au titre d'intérêts de retard : _____ €
- au titre de clause pénale : _____ €

Nous vous mettons dès lors en demeure de verser sous quinzaine la somme de _____ €, éventuellement majorée des intérêts journaliers complémentaires, sur mon compte de qualité BE_____, en précisant la référence _____.

À défaut de paiement pour le _____, cette somme devra encore être majorée d'un intérêt journalier de _____ €.

Vous pouvez obtenir, sur demande, toutes les pièces justificatives de la dette.

Notre cliente, si elle entend être payée, souhaite conserver votre relation commerciale.

Aussi, en cas de contestation de la dette, vous pouvez nous en adresser les motifs et pièces justificatives. Nous adresserons votre correspondance à notre cliente et nous reviendrons spontanément vers vous pour vous faire connaître sa position.

En tout état de cause, si vous devez faire choix d'un conseil, notre cliente vous invite à faire choix d'un avocat agréé en droit collaboratif dans la liste figurant sur la page <https://avocats.be/fr/tout-savoir/la-recherche-dune-solution-amiable>.

En effet, vous lirez sur la même page que le droit collaboratif est un processus de négociation volontaire et confidentiel aidant les parties à parvenir à une entente acceptable et durable pour chacune d'elles. Une solution permettant la poursuite de votre relation contractuelle pourrait donc être trouvée si vous faisiez choix d'un conseil formé à ce processus comme nous.

Si votre absence de paiement résulte de votre incapacité de payer le montant dû en une fois, vous pouvez demander des facilités de paiement. Nous communiquerons votre demande à notre cliente et nous reviendrons spontanément vers vous pour vous faire connaître sa position.

Cette lettre ne concerne PAS une citation au tribunal ou une saisie. Il ne s'agit pas d'une procédure de recouvrement judiciaire.

Toutefois, en l'absence de réaction dans le délai prévu à l'article XIX.9, § 1^{er} du Code de droit économique (un délai de quatorze jours calendrier prenant cours le troisième jour ouvrable qui suit celui de la présente mise en demeure), nous avons reçu mandat de recouvrer cette somme par voie judiciaire, sans nouveau rappel.

L'administration de surveillance de notre activité de recouvrement est le S.P.F. ÉCONOMIE, Direction Générale de la Réglementation économique, Service Crédit – Endettement, Rue du Progrès, 50 à 1210 BRUXELLES.

*

Vos données à caractère personnel (nom, prénom, profession, données de contact et financières, correspondances, pièces et actes de procédure) figurant sur les documents qui m'ont été remis et disponibles via les sources officielles sont traitées par _____ conformément au RGPD, en vue de la gestion de ce dossier, et ce sur base de nos obligations légales et de notre intérêt légitime, et celui de notre cliente, à défendre ses intérêts (articles 6.1.c et f) du RGPD).

Profession

Elles ne pourront être transmises que dans le respect de nos règles déontologiques, à notre cliente, aux juridictions, aux avocats collaborateurs chargés de ce dossier, aux autres parties intervenants dans ce dossier et aux auxiliaires de justice.

Ces données sont conservées pendant cinq ans après la clôture du dossier, durée pendant laquelle ma responsabilité professionnelle est susceptible d'être mise en cause.

Vous disposez, dans les limites prévues par le RGPD, du droit d'accéder à ces données, de demander leur rectification, la restriction de leur traitement, leur effacement et de vous opposer à leur traitement. Ces droits peuvent être exercés en vous adressant au délégué à la protection des données de _____ (_____). Une plainte peut le cas échéant être introduite auprès de l'Autorité de protection des données.

Pour plus de détails sur notre politique de protection de données : _____.

Nous vous prions de croire, Madame, à l'assurance de nos sentiments distingués.

Deepl Write

Formal notice by registered letter with receipt confirmed

Brussels, 27 May 2015

Your ref.: _____

Our ref.: _____

Dear Madam,

We are writing to you in our capacity as legal counsel for SA SOCIETE Y, whose registered office is located at _____, registered with the BCE under number _____ – Tel.: _____, email: _____.

You owe our client the sum of €_____ for unpaid invoices issued between May 2023 and April 2025, in accordance with a contract for the supply of heating oil. Due to your failure to pay within the contractual deadlines, your debt now amounts to €_____ in accordance with the following statement:

- Principal: €_____
- Late payment interest: _____ €
- Penalty clause: €_____

We hereby give you formal notice to pay the sum of €_____, plus any additional daily interest, into our account BE_____, quoting reference _____, within a fortnight.

If payment is not made by ___ ____, this sum will increase by daily interest of _____.

You can obtain all supporting documents relating to the debt upon request.

Our client wishes to maintain its business relationship with you, provided that it is paid.

Therefore, if you dispute the debt, please send us your reasons and supporting documents. We will forward your correspondence to our client, who will then contact you to inform you of their position.

If you decide to seek legal advice, our client invites you to choose a lawyer specialising in collaborative law from the list on the page <https://avocats.be/fr/tout-savoir/la-recherche-dune-solution-amiable>.

As you will see on the same page, collaborative law is a voluntary and confidential negotiation process that helps the parties reach an agreement that is acceptable and sustainable for all of them. Therefore, if you choose a lawyer trained in this process, such as ourselves, a solution that allows you to continue your contractual relationship could be found.

Profession

If you are unable to pay the amount owed in a single instalment, you may request payment facilities. We will forward your request to our client and contact you again to inform you of their response.

Please note that this letter does not concern a court summons or seizure. This is not a legal debt collection procedure.

However, if we do not receive a response within the time limit specified in Article XIX.9, §1 of the Economic Law Code (a period of fourteen calendar days starting on the third working day following the date of this formal notice), we will be instructed to recover this amount through legal proceedings without further notice.

The supervisory authority for our collection activities is the S.P.F. ÉCONOMIE, Direction Générale de la Réglementation Économique, Service Crédit – Endettement, Rue du Progrès, 50, 1210 Brussels.

*

Your personal data (surname, first name, profession, contact details, financial details, correspondence and procedural documents) appearing on the documents provided to me and available via official sources is processed by _____ in accordance with the GDPR for the purposes of managing this file, based on our legal obligations and our legitimate interests and those of our client to defend her interests (Articles 6.1.c and f of the GDPR).

This data may only be disclosed to our client, the courts, lawyers working on this case, other parties involved in this case and court officials, in accordance with our rules of professional conduct.

This data is kept for five years after the case is closed, during which time I may be held professionally liable.

Within the limits provided for by the GDPR, you have the right to access this data, request its rectification or erasure, restrict its processing or object to its processing. These rights may be exercised by contacting the data protection officer at _____ (______). If necessary, a complaint may be lodged with the Data Protection Authority.

For more details on our data protection policy, please visit: _____.

Yours faithfully,



Profession

ChatGPT

FORMAL NOTICE

BY REGISTERED MAIL WITH ACKNOWLEDGEMENT OF RECEIPT

Brussels, 27 May 2025

Your _____ Ref.: _____
Our _____ Ref.: _____

Dear Madam,

This letter is sent to you in our capacity as counsel for the company SOCIETE Y SA, whose registered office is located at _____, registered with the Crossroads Bank for Enterprises under number _____ – Tel.: _____ – Email: _____.

You are indebted to our client in the principal amount of €_____ for unpaid invoices issued between May 2023 and April 2025, pursuant to a fuel oil supply contract.

Due to your failure to make payment within the contractual deadlines, your debt has now increased to a total amount of €_____, broken down as follows:

- Principal: €_____
- Late payment interest: €_____
- Contractual penalty: €_____

We hereby give you **formal notice** to pay, within fifteen days, the sum of €, **possibly increased by additional daily interest, into our designated third-party account BE**, with the reference _____.

In the absence of payment by _____, this amount will be further increased by a daily interest of €_____.

All supporting documents relating to the debt are available upon request.

Although our client expects to be paid, it is keen to maintain its commercial relationship with you.

Therefore, if you contest the debt, you are invited to provide your reasons and supporting documents. We will forward your correspondence to our client and will revert to you with its position.

In any case, should you decide to seek legal counsel, our client recommends that you appoint a lawyer trained in collaborative law, as listed on the following webpage: <https://avocats.be/fr/tout-savoir/la-recherche-dune-solution-amiable>.

As you will read on that page, collaborative law is a voluntary and confidential negotiation process that helps the parties reach a mutually acceptable and sustainable agreement. Choosing an advisor trained in this process – as we are – could allow you to continue your contractual relationship with our client.

If your failure to pay is due to an inability to pay the full amount at once, you may request a payment plan. We will forward your request to our client and revert to you with its position.

This letter does NOT constitute a court summons or an attachment. It is not a judicial collection procedure.

However, in the absence of a reaction within the period provided for by Article XIX.9, §1 of the Belgian Code of Economic Law (a period of fourteen calendar days starting from the third working day after this formal notice), we are instructed to recover the amount through judicial proceedings, without further notice.

Our debt collection activity is supervised by: **FPS ECONOMY**, Directorate-General for Economic Regulation, Credit and Debt Service, Rue du Progrès 50, 1210 BRUSSELS.

Profession

Privacy Notice

Your personal data (name, first name, profession, contact and financial details, correspondence, documents, and procedural acts), contained in the documents provided to us and accessible through official sources, are processed by _____ in accordance with the GDPR, for the purpose of managing this case. This processing is based on our legal obligations and our legitimate interest, as well as that of our client, to defend its rights (Articles 6.1.c and f of the GDPR).

This data may only be shared, in compliance with our professional ethical rules, with our client, the courts, collaborating lawyers involved in this case, other parties to the case, and judicial officers.

The data will be retained for five years following the closure of the case, corresponding to the period during which our professional liability may still be engaged.

Within the limits provided by the GDPR, you have the right to access your data, request its rectification, restriction of processing, erasure, and to object to its processing. These rights may be exercised by contacting the Data Protection Officer of _____ (______). A complaint may also be filed with the Data Protection Authority.

For more details on our data protection policy: _____.

We
Yours sincerely,

remain,

Madam,

Le chat (Mistral)

REGISTERED LETTER WITH ACKNOWLEDGMENT OF RECEIPT

Brussels, May 27, 2015

Your ref.: _____

Our ref.: _____ - _____

Dear Madam,

This letter is sent to you in our capacity as counsel for the company SA SOCIETE Y, whose registered office is located at _____ _____, registered with the BCE under number _____ - Tel.: _____ - e-mail: _____.

You owe our client the principal amount of _____ € due to unpaid invoices, issued between May 2023 and April 2025, pursuant to a fuel oil supply contract.

Due to your failure to pay within the contractual deadlines, your debt now amounts to _____ € according to the following breakdown:

- Principal: _____ €
- Late payment interest: _____ €
- Penalty clause: _____ €

We hereby demand that you pay the amount of _____ €, possibly increased by additional daily interest, into my professional account BE_____, specifying the reference _____, within fifteen days.

In the event of non-payment by _____, this amount will be further increased by a daily interest of _____ €.

You can obtain, upon request, all supporting documents for the debt.

Our client, while wishing to be paid, wishes to maintain your business relationship.

If you dispute the debt, you can send us the reasons and supporting documents. We will forward your correspondence to our client and will spontaneously contact you to inform you of their position.

Profession

In any case, if you need to choose a counsel, our client invites you to choose a lawyer approved in collaborative law from the list on the page <https://avocats.be/fr/tout-savoir/la-recherche-dune-solution-amiable>.

Indeed, you will read on the same page that collaborative law is a voluntary and confidential negotiation process helping parties to reach an acceptable and sustainable agreement for each of them. A solution allowing the continuation of your contractual relationship could therefore be found if you choose a counsel trained in this process like us.

If your non-payment results from your inability to pay the amount due in one go, you can request payment facilities. We will communicate your request to our client and will spontaneously contact you to inform you of their position.

This letter does NOT concern a summons to court or a seizure. It is not a judicial recovery procedure.

However, in the absence of a response within the period provided for in Article XIX.9, §1 of the Code of Economic Law (a period of fourteen calendar days starting on the third working day following that of this formal notice), we have been mandated to recover this amount through judicial means, without further notice.

The supervisory authority for our recovery activity is the FPS ECONOMY, General Directorate of Economic Regulation, Credit – Debt Service, Rue du Progrès, 50 in 1210 BRUSSELS.

*

Your personal data (name, first name, profession, contact and financial data, correspondence, documents, and procedural acts) appearing on the documents provided to me and available via official sources are processed by _____ in accordance with the GDPR, for the management of this file, and this based on our legal obligations and our legitimate interest, and that of our client, to defend their interests (Articles 6.1.c and f) of the GDPR).

They may only be transmitted in compliance with our deontological rules, to our client, the courts, the collaborating lawyers in charge of this file, the other parties involved in this file, and the judicial officers.

These data are kept for five years after the closure of the file, a period during which my professional liability may be called into question.

You have, within the limits provided by the GDPR, the right to access these data, to request their rectification, the restriction of their processing, their erasure, and to object to their processing. These rights can be exercised by contacting the data protection officer of _____ (_____). A complaint can, if necessary, be lodged with the Data Protection Authority.

For more details on our data protection policy: _____.

We remain, Madam, yours faithfully."

Gemini

FORMAL NOTICE

BY REGISTERED MAIL WITH ACKNOWLEDGEMENT OF RECEIPT

Brussels, 27 May 2015

Your ref.: _____

Our ref.: _____ – _____

Dear Madam,

This letter is sent to you in our capacity as legal counsel for COMPANY Y PLC/SA, whose registered office is located at _____ _____, registered with the CBE (Crossroads Bank for Enterprises) under number _____ – Tel.: _____ – e-mail: _____.

Profession

You are indebted to our client for the principal sum of _____ € due to unpaid invoices, issued between May 2023 and April 2025, pursuant to a heating oil supply contract.

Due to your failure to pay within the contractual deadlines, your debt now amounts to the sum of _____ € according to the following breakdown:

- Principal: _____ €
- Late payment interest: _____ €
- Penalty clause: _____ €

We hereby formally demand that you pay the sum of _____ € within fifteen (15) days, potentially increased by additional daily interest, into my client account BE_____, quoting the reference _____.

In the event of non-payment by _____, this sum will be further increased by daily interest of _____ €.

You may, upon request, obtain all supporting documents for this debt.

Our client, while intending to be paid, wishes to maintain your business relationship.

Therefore, should you dispute the debt, you may provide us with the reasons and supporting documentation. We will forward your correspondence to our client and will promptly inform you of their position.

In any event, should you decide to seek legal counsel, our client invites you to choose a lawyer accredited in collaborative law from the list available at <https://avocats.be/fr/tout-savoir/la-recherche-dune-solution-amiable>.

Indeed, as you will see on the same page, collaborative law is a voluntary and confidential negotiation process that helps parties reach an agreement that is acceptable and sustainable for each of them. A solution allowing for the continuation of your contractual relationship could therefore be found if you were to choose counsel trained in this process, as we are.

If your non-payment is due to an inability to pay the outstanding amount in a single instalment, you may request a payment plan. We will communicate your request to our client and will promptly inform you of their position.

This letter does NOT constitute a court summons or a seizure. This is not a judicial debt recovery procedure.

However, in the absence of a response within the period stipulated in Article XIX.9, §1 of the Code of Economic Law (a period of fourteen calendar days commencing on the third working day following the date of this formal notice), we have been instructed to recover this sum through legal proceedings, without further notice.

The supervisory authority for our debt collection activities is the FPS ECONOMY, Directorate General for Economic Regulation, Credit and Debt Service, Rue du Progrès 50, 1210 BRUSSELS.

*

Your personal data (surname, first name, profession, contact and financial data, correspondence, supporting documents, and procedural documents) appearing on the documents provided to me and available via official sources are processed by _____ in accordance with the GDPR, for the management of this file, based on our legal obligations and our legitimate interest, and that of our client, in defending its interests (Articles 6.1.c and f) of the GDPR).

This data will only be transmitted in compliance with our professional rules of conduct, to our client, the courts, collaborating lawyers assigned to this file, other parties involved in this file, and judicial officers.

This data is retained for five years after the closure of the file, during which period my professional liability may be invoked.

You have, within the limits provided by the GDPR, the right to access this data, to request its rectification, the restriction of its processing, its erasure, and to object to its processing. These rights can be exercised by contacting the Data Protection Officer of _____ (_____). A complaint may, if necessary, be lodged with the Data Protection Authority.

For more details on our data protection policy: _____.

Yours faithfully,



Jonathan
Daniel

Substitut du procureur
du Roi de Charleroi
Magistrat de référence
en protection
des données



<https://www.linkedin.com/in/jonathan-daniel-charleroi/>

LE DÉVELOPPEMENT DE L'IA FACE AU RGPD : L'AVIS 28/2024 DU CEPD

Die Entwicklung der KI im Hinblick auf die DSGVO: Stellungnahme 28/2024 des EDSB

Am 17. Dezember 2024 antwortete der Europäische Datenschutzausschuss (EDSA) auf die Anfrage der irischen Aufsichtsbehörde und gab eine Stellungnahme zur Verarbeitung personenbezogener Daten im Rahmen der Entwicklungs- und Bereitstellungsphasen von Künstliche-Intelligenz-Modellen ab (Stellungnahme 28/2024). Diese Stellungnahme, die erste ihrer Art, erfolgt vor dem Hintergrund der raschen Entwicklung von KI-Technologien, während Rechtsexperten über die Datenschutzerfordernungen in Bezug auf diese neuen Instrumente diskutieren.

Trois questions avaient été posées par l'autorité irlandaise au CEPD, sur les thèmes suivants :

1. les conditions dans lesquelles un modèle d'IA peut être considéré comme « anonyme » ;
2. l'utilisation de l'intérêt légitime comme base juridique lors du développement et du déploiement d'un modèle d'IA ;
3. les conséquences d'un traitement illicite de données à caractère personnel pendant la phase de développement d'un modèle d'IA.

À titre liminaire

Avant d'évoquer ces trois questions, il convient de souligner la portée de l'avis. L'avis du CEPD se concentre sur les modèles d'IA, soit une notion non définie dans le règlement sur l'IA1. Selon le CEPD, un modèle d'IA est une composante essentielle d'un système IA mais non autonome. C'est un algorithme permettant de générer un résultat sur base de données qui lui sont communiquées, en vue de répondre à l'objectif prévu pour le système IA.

Par exemple, si le système IA a pour objectif de prédire les intentions d'achat des

En date du 17 décembre 2024, sur interpellation de l'autorité de contrôle irlandaise, le Comité européen de la protection des données (CEPD) a rendu un avis sur le traitement de données à caractère personnel dans le cadre des phases de développement et de déploiement des modèles d'intelligence artificielle (avis 28/2024). Cet avis, le premier en la matière, intervient dans un contexte de déploiement fulgurant des technologies d'IA, alors que les professionnels du droit s'interrogent sur les exigences du RGPD applicables à ces nouveaux outils.

1. Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle.



« L'intérêt légitime peut servir de base juridique. »

consommateurs, un modèle d'IA aura pour raison d'être d'étudier des données relatives aux achats réalisés par les consommateurs-cibles pour apprendre, comprendre et établir des concordances. L'avis s'intéresse précisément à ce type de modèles d'IA, qui analysent des données à caractère personnel².

L'absence de présomption d'anonymisation automatique des modèles d'IA

Sur la première question, le CEPD rejette la thèse selon laquelle un modèle d'IA, entraîné sur des données à caractère personnel, serait présumé anonyme une fois la phase de développement terminée³. Cette position, bien que prudente, complexifie évidemment l'exploitation des données, imposant une évaluation au cas par cas.

Celle-ci doit être réalisée, selon le CEPD, en tenant compte de la probabilité de pouvoir extraire des données à caractère personnel à partir du modèle, que ce soit directement ou via des requêtes.

Pour qu'un modèle soit considéré comme anonyme, la probabilité d'extraction de données personnelles doit être insignifiante, compte tenu de tous les moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou un tiers⁴.

Le CEPD propose une liste non exhaustive d'éléments pouvant permettre d'évaluer l'anonymisation du modèle, tels que la minimisation des données, la mise en place de tests de résistance

aux attaques ou la documentation des mesures prises pour limiter les risques d'identification.

L'intérêt légitime comme base juridique

Après un rappel de l'absence de hiérarchie entre les bases juridiques, l'avis précise que le consentement d'une personne n'est pas obligatoire pour l'usage des données dans le cadre d'un modèle d'IA.

L'intérêt légitime peut servir de base juridique uniquement si les trois conditions cumulatives suivantes sont remplies⁵ :

1. le responsable du traitement, ou un tiers, poursuit un intérêt légitime (licite, précis et actuel) ;
2. le traitement est nécessaire à la poursuite de l'intérêt légitime. Cette nécessité est analysée sous la lumière du principe de minimisation en se posant deux questions essentielles : le traitement est-il la poursuite de la finalité et, dans l'affirmative, n'existe-t-il de manière moins intrusive de poursuivre cette finalité ? ;
3. les intérêts ou les libertés et droits fondamentaux des personnes concernées ne prévalent pas sur l'intérêt légitime. Une mise en balance des intérêts en cause doit être réalisée, en tenant compte des mesures mises en place pour limiter l'impact sur le droit des personnes concernées.

Afin d'évaluer ce « test en trois étapes », tel que défini par le CEPD, différents critères d'évaluation ont été établis pour aider les autorités de contrôle dans leur tâche⁶.

Vu les propos tenus dans l'avis, il est clair que le choix de cette base juridique entraînera *de facto*, pour le responsable du traitement, une analyse complète et rigoureuse du traitement avant sa mise en fonction, sous peine d'entraîner une infraction au RGPD.

Les conséquences d'un traitement illicite lors du développement

La dernière question était relative aux conséquences d'un traitement illicite de données lors du développement du modèle d'IA. Après avoir rappelé qu'un traitement illicite peut être soumis à des mesures correctives de l'autorité de contrôle⁷, le CEPD précise qu'un tel traitement au stade du développement pourrait avoir une incidence sur la légalité lors de son déploiement. Les autorités de contrôle devront évaluer en tenant compte des circonstances de l'espèce la responsabilité de chaque acteur.

Seule exception à cette incidence : l'anonymisation complète après le développement et avant le déploiement. Dans cette hypothèse, le CEPD souligne que le RGPD ne s'applique pas au traitement réalisé lors du déploiement, à défaut de données à caractère personnel⁸, et le traitement illicite antérieur n'aura aucune incidence sur les activités postérieures, même si elles sont exercées par le même responsable de traitement.

L'avis du CEPD, une évolution du RGPD ?

Cet avis du CEPD apporte une approche ouverte et casuistique, cherchant à laisser une certaine marge de manœuvre aux différentes autorités

2. 2. P. 14 de l'avis.

3. 3. P. 16 de l'avis.

4. 4. L'avis fait référence, en sa p. 19, à l'arrêt CJUE du 19 octobre 2016, affaire C-582/14, *Breyer c. Bundesrepublik Deutschland*, ECLI:EU:C:2016:779, point 46, et à l'arrêt de la CJUE du 7 mars 2024, affaire C-479/22 P, *OC c. Commission européenne*, ECLI:EU:C:2024:215, point 51.

5. 5. P. 24 de l'avis, rappelant les arrêts CJUE, arrêt du 4 juillet 2023, affaire C-252/21, *Meta c. Bundeskartellamt*, ECLI:EU:C:2023:537, point 106 ; CJUE, arrêt du 11 décembre 2019, affaire C-708/18, *Asociația de Proprietari bloc M5A-ScaraA*, ECLI:EU:C:2019:1064, point 40.

6. 6. Voy. pp. 27 et s. de l'avis.

7. 7. Voir à des infractions pénales selon le cas (art. 222, 1° et 2°, de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel).

8. 8. À la p. 40 de l'avis, il est renvoyé au considérant 26 du RGPD.

de contrôle. Le CEPD ne manque pas de rappeler les obligations en vigueur aux différents acteurs du marché, mais reconnaît la complexité technique et les difficultés à assurer notamment une anonymisation effective. Les obligations du RGPD tendent à évoluer avec des technologies qui n'étaient pas imaginables lors de son élaboration.

Néanmoins, la doctrine⁹ reproche notamment au CEPD son manque de clarté et de précision pour les opérateurs du marché de l'IA pouvant être dissuasif, compte tenu des investissements à engager et des risques en cas de traitement considéré comme illicite.

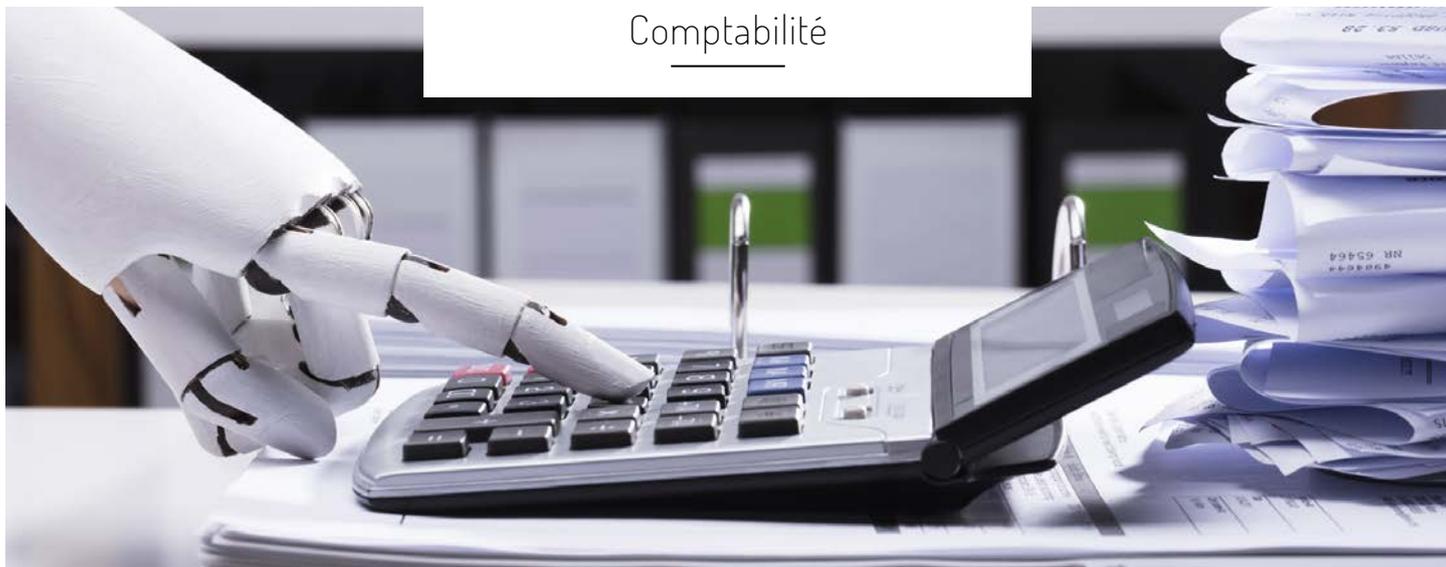
Cependant, comme le soulignent certains¹⁰, le CEPD n'avait pas réellement d'autre choix que de rejeter la thèse de l'anonymisation automatique, compte tenu des risques pour les personnes concernées, et de rédiger un avis pouvant s'adapter à cette technologie émergente et en constante évolution.

— Notre conseil

En définitive, l'avis du CEPD, en l'absence de prise de position figée, invite la profession à adopter une posture proactive, en intégrant la protection des données dès les premières étapes de la conception des projets d'IA.

2. 9. Voy. notamment J. CLARK, H. WAEM, J. MAGEE et R. DE SOUZA, « EU: EDPB Opinion on AI Provides Important Guidance though Many Questions Remain », in *Artificial Intelligence, EDBP (European Data Protection Board), Privacy Law*, 14 janvier 25.

2. 10. Voy. notamment S. STALLA-BOURDILLON et A. ROSSI, « A critical assessment of EDPB Opinion 28/2024: Towards a principle-based approach to innovation? », *Privacy and Data Protection*, 2025.



Joëlle
Van Hecke

Expert-comptable
et fiscal certifié ITAA
Associée cabinet Mats
Tax

<https://mats-tax.be/>

joelle@mats-tax.be



L'IA ET LA COMPTABILITÉ : AMIS, ENNEMIS OU PARTENAIRES ?

Künstliche Intelligenz und Buchhaltung Hand in Hand?

Es ist kein Geheimnis mehr, dass künstliche Intelligenz ein integraler Bestandteil unserer Arbeitswerkzeuge ist (oder wird) und die Bereiche, in denen sie uns unterstützen wird, immer zahlreicher werden.

Aber was kann sie uns für die Buchhaltung bringen?

Ce n'est plus un secret : l'intelligence artificielle fait partie intégrante de nos outils de travail et les domaines dans lesquels elle va nous épauler sont de plus en plus nombreux. Mais que peut-elle nous apporter pour la comptabilité ?

L'image du comptable qui additionne des chiffres dans un grand registre fait partie du passé depuis de nombreuses décennies.

L'ordinateur est venu aider le comptable dans son travail depuis longtemps et les logiciels comptables sont de plus en plus puissants et performants.

Mais aujourd'hui, il faut encore introduire de nombreuses données de manière manuelle dans ces programmes. L'IA peut donc, avec un certain succès, venir alléger une série de tâches comptables.

En comptabilité, toutes les conditions sont réunies pour pouvoir faire appel à l'intelligence artificielle : d'une part, un très grand nombre de données et, d'autre part, l'ordinateur qui va gérer ces données. C'est ici que l'informaticien a une mission essentielle à remplir : développer

les algorithmes qui vont trier, comparer et traiter les données.

Comment l'IA peut-elle intervenir dans un logiciel comptable ?

Prenons un exemple simple : une facture d'achat de fournitures de bureau.

L'IA peut identifier le numéro d'entreprise du fournisseur. En lien avec une base de données externe (la Banque Carrefour des Entreprises), le logiciel pourra créer automatiquement la fiche signalétique du fournisseur avec le nom, l'adresse, le numéro de TVA, le compte bancaire, etc.

Lors de la comptabilisation de la première facture de ce fournisseur, le comptable devra associer un compte comptable avec le fournisseur.



« L'intelligence artificielle peut dispenser le comptable de toute la partie "encodage". »

Par la suite, chaque fois qu'une facture de ce fournisseur sera téléchargée dans le logiciel, celui-ci ira vérifier comment elle a été traitée par le passé et va appliquer le même traitement. Le logiciel peut également reconnaître des informations telles que le montant TVA comprise, le montant hors TVA et le montant de la TVA. Une proposition de comptabilisation est alors générée par le logiciel et il suffit de confirmer celle-ci ou de la corriger.

Lors du paiement de la facture, le lien entre la fiche signalétique du fournisseur – qui reprend son numéro de compte bancaire – et le virement est réalisé de manière automatique. Le paiement est comptabilisé immédiatement sur le compte du fournisseur. De plus, avec la communication structurée indiquée sur la facture, le logiciel pourra relier directement le montant payé avec la facture correspondante.

À ce niveau, l'intelligence artificielle peut dispenser le comptable de toute la partie « encodage »,

extrêmement chronophage et source d'erreurs si l'intervention humaine y est liée.

L'IA peut-elle intervenir dans tous les logiciels comptables ?

Malheureusement non, car tout dépendra du logiciel comptable utilisé.

Il n'y a, à ce jour, que très peu de logiciels comptables qui intègrent une intelligence artificielle.

Un « vieux » logiciel ne pourra probablement pas traiter les données en utilisant l'intelligence artificielle et il faudra, dès lors, soit opter pour une version upgradée du programme, soit choisir un autre programme.

L'IA va-t-elle remplacer le comptable ?

Les professionnels du chiffre peuvent être rassurés : ils ont encore de belles missions à remplir.

Le programme pourra gérer des données, les traiter de manière plus rapide avec un risque très faible d'erreur, de nombreuses statistiques pourront être calculées, mais, même avec une intelligence artificielle très développée, seul un humain pourra correctement interpréter les chiffres de la comptabilité pour donner des conseils efficaces.

L'expert-comptable (certifié) a un rôle important à jouer en matière de conseil financier, conseil en gestion d'entreprises et, surtout, conseil fiscal. Son expertise et son expérience sont des atouts majeurs pour les entreprises.

Par ailleurs, *tout le temps qui sera économisé en utilisant l'intelligence artificielle pour le traitement des données sera du temps qui pourra être consacré à des missions de conseils à haute valeur ajoutée pour le cabinet d'avocats.*

Notre conseil

Nous l'avons rappelé dans un précédent numéro, la facture électronique Peppol sera bientôt obligatoire.

Saisissez l'opportunité de faire d'une pierre deux coups pour anticiper ces nouvelles obligations qui vont bouleverser nos cabinets : vérifiez dès à présent avec votre expert-comptable (certifié) si votre logiciel comptable est prêt pour affronter la digitalisation.

Optez pour un logiciel qui pourra gérer les factures électroniques, associé à une intelligence artificielle qui pourra les traiter de manière automatique.



Joëlle
Van Hecke

Expert-comptable
et fiscal certifié ITAA
Associée cabinet Mats
Tax

<https://mats-tax.be/>

joelle@mats-tax.be



NOUVEAUTÉS TVA « À PARTIR » DU 1^{er} JANVIER 2025 : L'ADMINISTRATION DE LA TVA PEINE À DÉVELOPPER LES NOUVEAUX OUTILS DIGITAUX ET DOIT REPORTER CERTAINES MESURES

MWSt-Neuheiten „ab“ 1. Januar 2025:

Die **Verwaltung** hat Schwierigkeiten, **neue digitale Werkzeuge** zu entwickeln und muss einige **Maßnahmen verschieben**

Die große Reform der „Mehrwertsteuerkette“ gerät ins Stocken. Die digitalen Werkzeuge, die es den Steuerpflichtigen ermöglichen sollen, die von der Mehrwertsteuerverwaltung zu erstattenden Beträge zu verwalten, werden nicht innerhalb der vorgesehenen Fristen fertiggestellt.

Zudem kritisieren Finanzdachleute einige Maßnahmen, die als zu belastend für die Steuerpflichtigen angesehen wurden.

Die Mehrwertsteuerverwaltung hat daher in einem Rundschreiben (Rundschreiben 2025/C/6 vom 27/01/2025) einige willkommene Präzisierungen – und Klarstellungen – vorgenommen.

In diesem Artikel analysieren wir die wichtigsten Punkte dieses Rundschreibens

Cette grande réforme de la « chaîne TVA » semble être compliquée à mettre en œuvre. Les outils digitaux qui devront permettre aux assujettis de gérer les sommes à rembourser par l'administration de la TVA ne seront pas prêts dans les délais prévus.

Les professionnels du chiffre ont également critiqué certaines mesures jugées trop contraignantes pour les assujettis. L'administration de la TVA a donc apporté certaines précisions – et clarifications bienvenues – dans une circulaire (Circulaire 2025/C/6 du 27 janvier 2025).

Nous analysons dans cet article les points les plus importants de cette circulaire.

1. Les nouveaux délais de dépôt des déclarations TVA

Auparavant, lorsque le délai fixé pour le dépôt de la déclaration TVA tombait un samedi, un dimanche ou un jour férié, la date ultime pour déposer la déclaration TVA – et payer le montant dû – était automatiquement reportée au premier jour ouvrable suivant.

La nouvelle législation entrée en vigueur le 1^{er} janvier 2025 supprimait cette tolérance de report au premier jour ouvrable suivant.

Par une communication du 22 novembre 2024, l'administration de la TVA annonçait une période transitoire pour la mise en œuvre progressive de la nouvelle réglementation jusqu'au 1^{er} mai 2025.

Dans la circulaire du 27 janvier 2025, l'administration de la TVA a prolongé la période transitoire jusqu'au 1^{er} octobre 2025.

Concrètement, cela signifie que, pour les déclarations TVA dont le délai de dépôt est antérieur au 1^{er} octobre 2025, il y a un report de la date ultime de dépôt (et de paiement) au premier jour ouvrable qui suit lorsque le 20 (déclaration TVA mensuelle) ou le 25 (déclaration TVA trimestrielle) est un samedi, un dimanche ou un jour férié. Exemple : le 20 juillet 2025 devient le 22 juillet 2025.

En revanche, pour les déclarations TVA dont le délai de dépôt est postérieur au 1^{er} octobre 2025, ce report au premier jour ouvrable suivant ne sera plus possible QUE pour les déclarations mensuelles et plus pour les déclarations trimestrielles.

Pour les assujettis déclarants mensuels, cette tolérance devient en fait permanente.

2. La tolérance des vacances d'été

Auparavant, les assujettis pouvaient déposer les déclarations TVA des mois de juin et juillet ou du 2^e trimestre au-delà du délai légal (au plus tard le 10 du mois suivant, sans report au premier jour ouvrable qui suit) sans être pénalisés pour un dépôt tardif.

Exemple : la déclaration TVA du 2^e trimestre 2024 pouvait être déposée jusqu'au 9 août 2024.

Ceci n'avait cependant aucun intérêt dans la réalité de terrain puisque le paiement de la TVA devait, lui, intervenir dans le délai « normal », à savoir pour le 20.

Par une communication du 22 novembre 2024, l'administration de la TVA annonçait avoir supprimé cette tolérance « vacances d'été » et appliquer le délai strict du 20 ou du 25.

Dans la circulaire du 27 janvier 2025, l'administration de la TVA a maintenu la tolérance « vacances d'été » mais uniquement pour l'année 2025.

3. La disparition du compte-courant TVA

Le compte-courant TVA, bien connu de tous les assujettis, devait être supprimé dans le cadre de la nouvelle réglementation pour être remplacé par un compte-provisions TVA.

Les services informatiques de l'administration TVA n'étaient cependant pas prêts et un report au 1^{er} mai 2025 a été annoncé.

Les travaux de développement des applications informatiques accusent un nouveau retard et un nouveau report au 1^{er} octobre 2025 a été décidé.

4. Une nouvelle procédure pour la restitution des crédits TVA

Pour rappel, à partir de 2025, une demande de remboursement (en cochant la case *ad hoc* de la déclaration TVA) ne concerne que l'excédent de la déclaration déposée dans le délai légal.

Si l'assujetti ne demande pas le remboursement (ou si les conditions pour obtenir ce remboursement ne sont pas remplies), le crédit TVA sera versé sur le compte-provisions. Pour pouvoir obtenir une restitution de ces montants, il faudra le demander explicitement via un instrument digital qui doit encore être développé par l'administration de la TVA. Le remboursement pourra être total ou partiel (l'assujetti déterminera lui-même le montant).

La disposition de report au 1^{er} octobre 2025 est applicable également à la nouvelle procédure de demande de remboursement des sommes en faveur des assujettis, pour les mêmes motifs de retard dans les travaux de développement des outils informatiques.

5. Les nouvelles amendes

Nous rappelons ci-dessous le montant des nouvelles amendes – salées – prévues à partir du 1^{er} janvier 2025 :

Pour le non-dépôt d'une déclaration :

- 1^{re} infraction : **500 €** par déclaration
- 2^e infraction : **1 250 €** par déclaration
- 3^e infraction : **2 500 €** par déclaration
- À partir de la 4^e infraction : **5 000 €** par infraction

Le délai de « remise à zéro » est particulièrement long : pour déterminer le montant de l'amende à appliquer, il sera tenu compte des infractions identiques commises au cours de la

période de quatre ans qui précède le moment où l'infraction sera commise.

Exemple : infraction commise en décembre 2026 et nouvelle infraction en août 2030 → en août 2030, la période de quatre ans n'est pas encore écoulée et il s'agira alors de la 2^e infraction.

Pour un dépôt tardif :

- 100 € par déclaration et par mois de retard
- Chaque mois entamé vaut pour un mois entier
- Avec un maximum de 500 €

Un adoucissement a été prévu pour l'assujetti de bonne foi qui déposera tardivement une déclaration TVA.

Lorsque la déclaration TVA est déposée au plus tard le 10^e jour du 2^e mois qui suit la période de déclaration :

- déclarations dont le délai légal de dépôt est antérieur au 1^{er} octobre 2025 → aucune amende ne sera infligée ;
- déclarations dont le délai légal de dépôt est postérieur au 1^{er} octobre 2025 → la première infraction commise de bonne foi sera entièrement remise, mais uniquement lorsqu'une requête sera introduite pour demander cette remise.

Cette tolérance deviendra permanente, mais ne sera valable que pour l'amende pour dépôt tardif.

L'attention de l'assujetti est attirée sur le fait que la remise ne sera pas accordée automatiquement : une requête motivée (en remise d'amendes en application de l'arrêté du Régent) devra être introduite. Il s'agit, d'une part, d'une formalité supplémentaire et qui, d'autre part, sera généralement facturée par l'expert-comptable (certifié) si celui-ci est mandaté pour cette mission.

Notre conseil

Le retard dans le développement, par l'administration de la TVA, des outils informatiques qui doivent simplifier la vie des assujettis permet d'obtenir un délai supplémentaire pour s'adapter à cette nouvelle réglementation.

Les retardataires et mauvais payeurs sont définitivement dans le viseur de l'administration TVA et même la bonne foi ne sera pas présumée.

Prenez vos dispositions pour respecter les délais de dépôts et de paiements pour éviter les sanctions.

Votre expert-comptable (certifié) reste à votre disposition pour vous accompagner dans cette transition.

Agenda



14-15 juillet 2025

IBA, Building the Law Firm of The Future, Varsovie, Pologne

→ <https://www.ibanet.org/conference-details/CONF2609>



22-25 juillet 2025

IBA Law Firm Management Committee Academy for Leaders, Londres, Royaume-Uni

→ <https://www.ibanet.org/conference-details/CONF2602>



16 septembre

Larciér-Intersentia – Rédiger des avis juridiques créateurs de valeur – Webinaire

→ <https://www.larciér-intersentia.com/fr/webinaire-rediger-avis-juridiques-createurs-valeur-ev0000245.html>



2-7 novembre 2025

IBA – Congrès annuel – Toronto, Canada

→ <https://www.ibanet.org/>



29 octobre-2 novembre 2025

UIA – Congrès annuel – Guadalajara, Mexique

→ <https://www.uianet.org/fr/evenements/69e-congres>



3-5 décembre 2025

CIB – Congrès annuel (des 40 ans!) – Lomé, Togo

→ <https://www.cib-avocats.org/congres-de-lome-2025>

Sommaire

Rédacteur en chef | *Chefredakteur*

Jean-François Henrotte, Avocat / Rechtsanwalt

Secrétaire de rédaction | *Redaktionssekretär*

Aurélien Bortolotti, Avocat / Rechtsanwalt

Comité de rédaction belge |

Redaktionsausschuss Belgischer

Alexandre Cassart, Avocat / Rechtsanwalt

Pauline Monforti, Avocate / Rechtsanwältin

Robert De Baerdemaeker, Avocat / Rechtsanwalt

Anne Delrue, Experte-comptable /

Wirtschaftsprüferin

Olivier Haenecour, Avocat / Rechtsanwalt

Johannes Seel, Avocat / Rechtsanwalt

Joëlle Van Hecke, Experte-comptable /

Wirtschaftsprüferin

www.managinglawyer.be

Comité de rédaction luxembourgeois |

Redaktionsausschuss Luxemburg

Rosario Grasso, Avocat / Rechtsanwalt

Nicolas Thieltsen, Avocat / Rechtsanwalt

www.managinglawyer.lu

Éditeur responsable | *Verantwortlicher Herausgeber*

Paul-Etienne Pimont, ELS Belgium s.a.

Avenue Jean Monnet, 4 | 1348 Louvain-la-Neuve

Régie publicitaire | *Werbeagentur*

LTH Consulting

Laurence Thomsin

Mobile: 0032 471 63 67 01

E-mail : laurencethomsin@gmail.com



LARCIER
INTERSENTIA

- 1 Intelligence artificielle en cabinet d'avocat(e)s, entre prudence et nécessaire innovation
Künstliche Intelligenz in Anwaltskanzleien: Zwischen Vorsicht und notwendiger Innovation
Jean-François Henrotte
- 3 L'intégration de l'intelligence artificielle dans la profession d'avocat : enjeux juridiques et déontologiques
Die Integration von künstlicher Intelligenz in den Anwaltsberuf: rechtliche und deontologische Herausforderungen
Cynthia Chartier et Jeffrey Vigneron
- 10 Stagiaires et intelligence artificielle : opportunités, vigilance et encadrement par les maîtres de stage
Praktikanten und künstliche Intelligenz: Chancen, Prinzipien und Betreuung durch Praktikumsleiter
Florence Garcet
- 13 Est-ce une bonne idée pour les avocats d'utiliser l'intelligence artificielle dans leur marketing ?
Ist es eine gute Idee für Anwälte, künstliche Intelligenz in ihrem Marketing einzusetzen?
Anne-Laure Losseau
- 16 Les journalistes de la RTBF face à l'essor de l'intelligence artificielle
Die Journalisten des RTBF und der Einzug der künstlichen Intelligenz
Aurélie Didier
- 20 Cybersécurité : un impératif également pour les cabinets d'avocat(e)s
Cybersicherheit: auch für Anwaltskanzleien ein Muss!
Axel Beelen et Jeffrey Vigneron
- 25 L'attitude du client et de la cliente final(e) face aux nouvelles technologies : leçons tirées d'une étude belge
Die Einstellung des Mandanten zu neuen Technologien: Erkenntnisse aus einer belgischen Studie
Johannes Seel
- 28 La justice du sens : l'IA au service de la traduction
KI im Dienste der Übersetzung
Jean-François Henrotte
- 36 Le développement de l'IA face au RGPD : l'avis 28/2024 du CEPD
Die Entwicklung der KI im Hinblick auf die DSGVO: Stellungnahme 28/2024 des EDSB
Jonathan Daniel
- 39 L'IA et la comptabilité : amis, ennemis ou partenaires ?
Künstliche Intelligenz und Buchhaltung Hand in Hand?
Joëlle Van Hecke
- 41 Nouveautés TVA « à partir » du 1^{er} janvier 2025 : l'administration de la TVA peine à développer les nouveaux outils digitaux et doit reporter certaines mesures
MwSt-Neuheiten „ab“ 1. Januar 2025: Die Verwaltung hat Schwierigkeiten, neue digitale Werkzeuge zu entwickeln und muss einige Maßnahmen verschieben
Joëlle Van Hecke
- 44 Agenda

Vous souhaitez recevoir la version numérique de *Managing Lawyer* ?

Abonnez-vous gratuitement à notre newsletter en remplissant le formulaire en ligne sur <https://www.larcier-intersentia.com/fr/managing-lawyer-abonnement>

Ou scannez directement le QR Code avec votre smartphone.



LARCIER
INTERSENTIA
LEFEBVRE GROUP

FORMATION

EN PRÉSENTIEL



Assistant(e)s en cabinet d'avocat(e)s : les clés du métier

Vendredi 7 novembre 2025 | Bruxelles

PRÉSENTATION

Vous êtes avocat(e) et vous avez à vos côtés un(e) assistant(e) ou un(e) secrétaire ?

La mission d'un(e) secrétaire ou d'un(e) assistant(e) juridique, au sein d'un cabinet d'avocat(e)s est la clé de voûte de bien des aspects relatifs à la bonne gestion de votre activité. Malgré ses qualités relationnelles et organisationnelles, vous avez peut-être remarqué qu'il lui reste certaines interrogations :

Comment optimiser la communication au sein du cabinet et sa position au sein de celui-ci ? Quelles sont les règles d'or de base à mettre en place pour protéger le cabinet des cyberattaques ? Quel est son rôle par rapport à la lutte contre le blanchiment des capitaux et le financement du terrorisme face au nouveau corpus réglementaire ? L'intelligence artificielle peut-elle l'aider dans la digitalisation et le traitement des documents ?

Voilà toute une série de questions auxquelles votre assistant(e)/secrétaire trouvera réponse ! En une matinée, un panel de professionnels y répondra.

L'après-midi sera réservée à un atelier pratique, au choix :

- « L'intelligence artificielle : l'art du prompting »
- « Dire et écrire le droit en français correct »

Découvrez le programme complet sur notre site [larcier-intersentia.com](https://www.larcier-intersentia.com)

INFORMATIONS PRATIQUES

Date et horaire

Vendredi 7 novembre 2025, de 9h15 à 16h30

Lieu

Bip - Maison de la Région - Rue Royale, 2-4 - 1000 Bruxelles

Accès

À 5 minutes à pied de la gare centrale
Metro 1, 5 (arrêt Gare Centrale ou Parc) -
Bus 38, 71, 95 (arrêt Royale)

Prix

215,00 € TTC : Participation à la matinée
360,00 € TTC : Participation à la matinée + à un atelier au choix
+ sandwiches à midi

Documentation

Les participants recevront la documentation préparée par les orateurs. Certaines présentations ne seront pas accompagnées de documentation.

Public visé

Secrétaire et assistant(e) exerçant une fonction au sein d'un cabinet d'avocat(e)s.

Renseignements complémentaires

Larcier - Intersentia
formations@larcier-intersentia.com
Numéro gratuit : 0800 39 067

