Responsabilité dans le développement et la distribution de l'intelligence artificielle en Allemagne - un #FernerLegalPaper de l'avocat Jens Ferner, spécialiste du droit informatique et du droit pénal

- Introduction
- Responsabilité du fait des produits
  - Influence des lois de protection
  - La responsabilité du fait des produits pensée différemment
- Particularités contractuelles
  - Négligence
  - Conditions contractuelles
  - obligation de mise à jour
  - discrimination
  - Développement de logiciels
- Particularités du droit du travail
- Particularités du marketing
  - Chatbots
  - Agences de publicité
  - Loi sur les services numériques
- Responsabilité de la direction
- Obligation d'indemnisation des fournisseurs d'IA
- Perspectives
- Conclusion et recommandation d'action
- À propos de l'auteur et du cabinet

Introduction

Après que le thème de l'intelligence artificielle soit devenu très soudainement partie intégrante du quotidien pratique de la plupart des gens, la question de la responsabilité a certes été rapidement mise en avant ; toutefois, on s'est très vite concentré sur l'AI-Act européen, le règlement sur l'IA, qui avance certes lentement mais sans garantie d'issue.

En réalité, il existe des règles nationales sur la responsabilité - ou plutôt les responsabilités - dans le développement et la distribution de l'intelligence artificielle. Le cadre juridique existant jusqu'à présent doit être esquissé dans ce résumé lâche afin d'illustrer les énormes obligations qui sont déjà en jeu aujourd'hui.

Responsabilité du fait des produits

La responsabilité du fait des produits est un domaine très vaste, qui englobe notamment les logiciels. En Allemagne, il convient de mentionner la loi sur la responsabilité du fait des produits, qui transpose la directive européenne sur la responsabilité du fait des produits et prévoit des droits indépendants de la faute. En outre, il existe dans le droit civil national, le Code civil (BGB), des dispositions qui créent des droits pour les personnes concernées en fonction de la faute.

```
Il convient de mentionner qu'il existe une controverse sur la question de
savoir si les logiciels sont couverts par la loi sur la responsabilité du
fait des produits, ce qui est en tout cas affirmé pour les logiciels livrés
dans du matériel. De notre point de vue, cette controverse est dépassée sur
le fond, la majorité de la littérature considère qu'il y a responsabilité
du fait des produits. De plus, dans un avenir proche, une nouvelle
directive européenne sur la responsabilité du fait des produits influencera
les lois nationales, dans laquelle le logiciel en tant que tel est
expressément prévu. On devrait donc impérativement s'y intéresser en tant
que fabricant d'IA !
```

Même si l'IA est une nouvelle application, il s'agit en fin de compte d'un logiciel et il est incontestable que toutes les réflexions menées jusqu'à présent sur la responsabilité s'appliquent à la distribution de logiciels. Selon la situation juridique actuelle, un comportement erroné d'une IA doit déjà être pris en compte comme indice d'un défaut du produit, en particulier si l'écart de comportement par rapport au comportement souhaité peut encore être reproduit.

Si l'on s'intéresse à la responsabilité du fait des produits au sens large, il faudra ainsi garder à l'esprit les thèmes suivants :

1. conception et fabrication : les erreurs de fabrication doivent être évitées lors de la création de systèmes d'IA, notamment lors de la formation. Cela signifie que les sources de connaissances généralement disponibles doivent être prises en compte dès la "fabrication" d'une IA afin d'éviter tout risque ultérieur. Un contrôle de qualité des données d'entraînement de l'IA devrait dans tous les cas en faire partie. Le critère de diligence se mesure en fin de compte à la question de savoir si le fabricant devait avoir connaissance d'un défaut lors de la mise en circulation du produit, c'est-à-dire de l'IA. En revanche, si une erreur ne s'avère être telle que plus tard, on parlera d'une "erreur de développement" qui ne se répercute qu'au niveau de l'observation du marché.
   2) **Instruction** : même si cela ne figure pas concrètement quelque part dans la loi, il incombe au fabricant du produit de veiller, par des instructions appropriées, à ce que l'acquéreur puisse utiliser le système conformément à sa destination. Les obligations concrètes dépendent tout particulièrement du canal de distribution, du groupe cible attendu et de l'utilisation erronée à laquelle on peut objectivement s'attendre. Selon la jurisprudence de la Cour fédérale de justice, il n'est pas possible d'abaisser le niveau de diligence en se contentant d'étiqueter le groupe cible. Celui qui vend à des consommateurs finaux, par exemple via un site web librement disponible, et qui écrit dans le mode d'emploi que seuls des utilisateurs professionnels doivent utiliser le logiciel, ne sera pas entendu si un profane provoque des dommages par une mauvaise utilisation.
   3) **Surveillance du marché** : la surveillance du marché est une obligation que les petits fournisseurs ont tendance à sous-estimer et qui doit être prise au sérieux de toute urgence. Il ne s'agit en aucun cas de se contenter de recueillir et d'évaluer les commentaires des clients. En outre, il faut au moins jeter un coup d'œil à la littérature spécialisée actuelle et il existe même une jurisprudence en Allemagne selon laquelle l'interaction avec les produits d'autres fabricants doit

être observée et prise en compte. Si un produit d'IA est conçu pour fonctionner comme un composant d'un autre logiciel, il faut veiller à ce que l'interaction entre les deux produits soit également prise en compte.

Influence des lois de protection

En plus de la responsabilité fondamentale du fait des produits ou des producteurs, un autre aspect intervient dans le droit civil allemand : si un dommage survient en raison de la violation d'une loi visant à protéger les personnes, ce dommage peut également faire l'objet d'une demande d'indemnisation. Ce qu'il faut considérer comme une loi de protection dans ce sens est loin d'être toujours clair, d'autant plus qu'il n'y a guère de jurisprudence à ce sujet jusqu'à présent. Par exemple, il n'est absolument pas clair si les exigences en matière de sécurité des logiciels dans le cadre du Cyber Resilience Act et de la législation nationale progressive sur la sécurité informatique entrent dans cette catégorie. Où "pas clair" signifie qu'il existe ici un potentiel de responsabilité considérable avec lequel il ne faut pas jouer au poker ! La situation juridique actuellement floue existe également, selon notre avis, dans la loi sur la sécurité des produits, où un logiciel peut, selon les cas, être un produit. Dans ce cas, un logiciel utilisé pour commander une machine - et qui fait partie intégrante de cette machine - doit être considéré dans le cadre de l'évaluation des risques conformément au règlement sur les machines (9e ProdSV).

La responsabilité du fait des produits pensée différemment

La responsabilité esquissée ici sommairement peut avoir des conséquences très surprenantes en droit allemand : Ainsi, selon la nouvelle jurisprudence de la Cour suprême, un mandataire au sens de la loi sur la sécurité des produits peut être tenu pour responsable, en tant que complice ou perturbateur, des violations des droits de protection causées par la mise en circulation du produit par le fabricant.

Il faut donc garder à l'esprit, lors de la commercialisation de l'IA, qu'il ne s'agit pas uniquement de logiciels défectueux au sens fonctionnel, mais que la responsabilité en Allemagne est également menacée par des détours, en particulier dans le domaine des droits de propriété intellectuelle, là où on ne peut pas les reconnaître d'emblée.

```
Dans ce contexte, la mise en danger du crédit constitue une particularité :
Celui qui, contrairement à la vérité, affirme ou diffuse un fait de nature
à compromettre le crédit d'autrui ou à lui porter préjudice d'une autre
manière dans son acquisition ou son avancement, est tenu de réparer le
dommage qui en résulte pour autrui, même s'il ne connaissait pas la
fausseté, mais devait la connaître. Il y a certainement là un champ
d'action considérable en rapport avec le traitement automatisé
d'informations ayant des répercussions sur des personnes individuelles !
```

Particularités contractuelles

Les particularités contractuelles qui en résultent dépendent de la structure de la distribution. Ainsi, les accords contractuels sont nettement plus difficiles à conclure avec les consommateurs, alors que la marge de manœuvre contractuelle est au moins un peu plus grande avec les clients professionnels.

Négligence

Tout d'abord, vous devez savoir qu'en Allemagne, la **négligence** est définie très simplement par la loi : agit de manière négligente celui qui ne fait pas preuve de la diligence requise dans le trafic. Il s'agit là d'une définition très large, qui invite à prévoir des aménagements contractuels appropriés - celui qui ne le fait pas est responsable de toute violation de l'obligation de diligence en cas de prestation défectueuse ! Mais en même temps, le droit civil allemand impose un contrôle extrême des conditions contractuelles préformulées, conformément au droit européen.

Conditions contractuelles

Ainsi, les dispositions des **conditions générales** sont nulles si elles désavantagent de manière déraisonnable le partenaire contractuel de l'utilisateur, contrairement aux règles de la bonne foi. La loi dresse une liste des conditions contractuelles

interdites aux consommateurs. Avec cette évaluation législative claire, il n'est pas possible de facto de prévoir en Allemagne une exclusion de responsabilité complète ou une limitation de responsabilité très restrictive en termes de montant. Le principe du tout ou rien s'applique : si une clause est invalide, il n'y a pas de possibilité de la sauver, par exemple en la comprenant comme la loi le permettrait. Avec la Cour fédérale de justice, une clause invalide ne peut pas être sauvée, en tout cas pour les consommateurs !

obligation de mise à jour

Un autre aspect est l'**obligation de mise à jour** : celle-ci a été introduite dans le droit civil allemand en 2022, se base sur des prescriptions de l'UE et est actuellement peu claire à bien des égards. Ce qui est certain, c'est que si une IA est mise sur le marché en tant que produit numérique, elle est soumise d'une part au droit des défauts matériels. Le droit moderne des défauts matériels, c'est-à-dire la question de savoir quand un produit présente un défaut au sens juridique du terme, a été développé : Il est impératif de déterminer objectivement si le logiciel présente un défaut, indépendamment de ce qui a été convenu dans le contrat. Il peut donc arriver qu'un défaut soit soudainement supposé en dehors de ce qui a été clairement convenu. En outre, une obligation de mise à jour obligatoire est prévue. Que le produit numérique soit mis à disposition "en tant que service" ou qu'il soit acheté une seule fois, ce qui est de moins en moins courant, une mise à jour à long terme du logiciel est due. Cela s'appliquera également aux données d'entraînement, de sorte que les bases de données vectorielles, par exemple, devront être mises à jour.

discrimination

La prochaine particularité du droit des contrats est la prévention de la **discrimination** : en Allemagne, il existe la "loi générale sur l'égalité de traitement", qui vise d'une part à empêcher la discrimination dans le cadre des relations de travail. Mais en même temps, cette loi stipule que, dans les contrats, les

- sont typiquement conclues sans considération de la personne, à des conditions comparables dans un grand nombre de cas (transactions de masse) ou
- pour lesquelles la réputation de la personne n'a qu'une importance secondaire en raison de la nature de l'obligation et qui sont conclues à des conditions

comparables dans un grand nombre de cas

aucune discrimination ne doit avoir lieu. Une infraction s'accompagne d'obligations de dédommagement. Il existe ici un risque de responsabilité considérable lorsqu'une IA doit par exemple exécuter des commandes de manière automatisée et tente de conclure ou de refuser des contrats en fonction de la solvabilité déterminée de manière automatisée. Il convient de rappeler brièvement qu'une telle procédure de refus automatique de contrat est déjà inadmissible du point de vue de la protection des données.

Développement de logiciels

Le **développement de logiciels** doit également être considéré d'un œil critique : Les contenus générés par l'IA ne sont, en tout cas dans l'état actuel des choses, pas protégés par des droits de propriété industrielle, notamment par le droit d'auteur. Parallèlement, les solutions de programmation basées sur l'IA sont largement répandues depuis des années.

En tout cas, les solutions simples pour compléter automatiquement les entrées ne devraient pas poser de problème, tout comme les environnements de test automatisés. Mais si des solutions complètes sont utilisées pour formuler des sections entières de code, celles-ci devraient finalement être qualifiées de domaine public. Le réveil est brutal lorsque des droits d'utilisation étendus sont néanmoins accordés sans réflexion dans les contrats, ce qui n'est pas possible pour une œuvre du domaine public. Là aussi, un scénario de responsabilité peut se présenter, du moins en théorie.

Particularités du droit du travail

En Allemagne, le droit du travail est imprégné d'une idée de protection considérable en faveur de l'employé - ce qui surprend toujours les employeurs étrangers, surtout lorsque l'on constate à quel point il est difficile de licencier dans ce pays. Cette idée de protection joue également un rôle important dans le traitement des données des employés, y compris lorsqu'il s'agit du traitement des données par l'IA. Le droit

allemand manque d'une législation clairement structurée en matière de protection des données des travailleurs. Il faut se contenter du RGPD et d'une clause générale dans le droit allemand de la protection des données.

En principe, le **traitement des données** des candidats par des logiciels, y compris l'IA, peut être fondé sur cette clause générale. En revanche, il convient d'être plus prudent lorsque des données sont collectées et traitées sans que la candidature ait été déposée ; dans ce cas, il est vivement déconseillé de collecter des données de manière forcée, par exemple à partir de profils de médias sociaux ! En raison de l'idée de protection du droit du travail, il n'est pas possible de faire des déclarations générales concernant les candidats : En principe, la collecte et le traitement de données par les candidats sont possibles et autorisés, mais plus le processus de traitement a un impact sur les droits de la personnalité du candidat, plus il doit être considéré de manière critique.

Ces idées restent valables dans le cadre des relations de travail existantes, où il faudra également peser les intérêts lors de l'utilisation de l'IA. Les intérêts fondamentaux de l'employeur (utilisation de l'IA) et de l'employé (protection des droits de la personnalité) doivent être mis en balance au cas par cas. Ainsi, des mesures de contrôle des employés peuvent notamment être autorisées, divers facteurs pouvant jouer un rôle, notamment la fréquence et la profondeur des traitements de données ainsi que le caractère potentiellement erroné et la possibilité de se prémunir efficacement contre les erreurs. Le droit allemand se révèle parfois imprévisible à cet égard, par exemple lorsque des mesures de surveillance étendues étaient autorisées chez un vendeur par correspondance sur Internet, mais que l'enregistrement biométrique du temps de travail a été rejeté comme étant illicite.

```
D'où la remarque suivante : dans le droit du travail allemand, méfiez-vous
des déclarations trop générales ! En raison de l'évaluation qui doit
toujours être faite en tenant compte de toutes les circonstances concrètes,
il se peut qu'une solution soit utilisée de manière autorisée par un
employeur et pas par un autre. S'il ne s'agit pas de solutions minimales,
on ne peut faire que des déclarations limitées sans le scénario
d'utilisation concret.
```

La **discrimination** des travailleurs et des candidats constitue un autre domaine thématique dans l'environnement du droit du travail. Dans ce domaine, il convient de rappeler la loi générale sur l'égalité de traitement dont il a déjà été question : Celle-ci prévoit un allègement considérable des preuves en ce sens qu'il suffit de présenter des indices qui parlent en faveur d'une discrimination. Certaines questions ou une analyse linguistique peuvent parfois suffire - mais aussi le processus de sélection dans son ensemble et les candidats sélectionnés à la fin. Un scénario catastrophe dans ce contexte serait par exemple un chatbot mal formé qui poserait des questions inadmissibles (par exemple sur l'âge, la grossesse ou les enfants souhaités dans le futur). Dans ce cas, les employés (potentiels) peuvent demander des dommages et intérêts. D'autre part, il existe également des demandes de recours contre les développeurs ou les fournisseurs d'IA.

C'est précisément lors de l'utilisation de l'IA dans le droit du travail qu'il faut tenir compte des **conditions complexes en matière de protection des données** : Ainsi, il existe une interdiction de principe des décisions purement automatisées. Si une IA effectue par exemple une observation des employés et prononce de manière automatisée un blâme pour un comportement fautif ou une modification de l'activité de travail, cela n'est pas autorisé.

En outre, il est prévisible que la plupart des employeurs n'utiliseront justement pas de solution individuelle sur place, mais achèteront une solution en nuage ("IA as a Service"). Dans ce cas, les problèmes classiques de protection des données doivent être pris en compte, en particulier, ce serait un désastre si les données des employés étaient stockées en dehors de l'UE sans contrôle juridique (ou si l'on ne sait pas clairement où cela se passe) ; le "traitement des commandes" doit également jouer un rôle lors de l'installation de tels produits d'IA, sachant qu'il y aurait probablement une "responsabilité partagée" lors de l'utilisation des données des employés pour la formation des systèmes d'IA, ce qui impliquerait des obligations considérables pour le fournisseur d'IA. Enfin, une analyse d'impact sur la protection des données sera nécessaire, ce qui semble difficilement envisageable sans la divulgation des principes de fonctionnement de l'IA.

Pour conclure, il convient de rappeler que dans les grandes entreprises en Allemagne, il faut tenir compte des droits du comité d'entreprise, qui peut avoir des droits de codécision dans un grand nombre de scénarios. Ici aussi, les fournisseurs étrangers sont souvent surpris, par exemple lorsqu'on considère qu'un droit de codécision peut découler de la protection de la santé sous l'aspect qu'un contrôle permanent - même supposé - par une IA représente une charge mentale. Quoi qu'il

en soit, un droit de codécision du comité d'entreprise est obligatoirement prévu lors de l'introduction et de l'utilisation de dispositifs techniques, de sorte qu'il est peu probable qu'une IA sérieusement mise en œuvre le soit sans comité d'entreprise.

Particularités du marketing

La responsabilité en matière de protection des données ne devrait pas non plus être sous-estimée dans le marketing. Nous nous concentrons ici délibérément sur les aspects du marketing - nous supposons que les aspects du droit de la personnalité et de la protection des données jouent un rôle dans l'entraînement de l'IA, et qu'une présentation indépendante serait déjà extrêmement complète.

Chatbots

De l'avis unanime, il faudra procéder à une évaluation des conséquences en matière de protection des données au sens du RGPD, en particulier lors de l'exploitation de chatbots et d'assistants de communication similaires. En outre, il faudra examiner la forme du consentement de plus près que ce qui a été constaté jusqu'à présent sur les sites web : de ce point de vue, il existe des doutes considérables quant à la suffisance du système traditionnel d'une déclaration de protection des données qui est simplement reliée par un lien. La littérature spécialisée souligne à juste titre que, premièrement, le consentement doit être obtenu dans le cadre de l'outil de communication lui-même (par exemple dans la fenêtre du chatbot) et que, deuxièmement, le consentement doit être obtenu dans le cadre de l'outil de communication lui-même (par exemple dans la fenêtre du chatbot).

Il conviendra d'accorder une attention particulière aux questions de profilage, aux comportements d'entraînement éventuels et aux saisies surprises des utilisateurs. Concernant ce dernier point, il convient de rappeler que les utilisateurs peuvent également saisir des catégories particulières de données à caractère personnel ou des données à caractère personnel de tiers de manière non planifiée. Un point positif est que, selon la jurisprudence actuelle de la Cour de justice de l'UE, un traitement de données non conforme ne suffit pas à lui seul à déclencher une

demande de dommages et intérêts. Toutefois, la jurisprudence allemande donne naissance à des droits d'abstention indépendants de la faute, qui peuvent être revendiqués avec d'autres frais. A cela s'ajoute le risque d'amendes.

Agences de publicité

Actuellement, l'attitude des agences de publicité n'est pas claire : selon la jurisprudence allemande actuelle, les agences de publicité doivent informer leurs clients, du moins en principe, de la nécessité d'un conseil juridique. Cela vaut même dans des domaines exigeants comme le droit des marques, si cela est méconnu, l'agence de publicité risque d'être responsable. Si une agence est chargée de la mise en place d'un outil d'intelligence artificielle pour la création de profils ou la communication avec les clients, on peut s'attendre à ce qu'il existe également dans ce cas une obligation d'information vis-à-vis du client - et qu'en cas de manquement, l'obligation d'indemnisation vis-à-vis du client soit en jeu.

Loi sur les services numériques

Pour conclure, il convient de souligner que les grands modèles linguistiques (LLM) sont soumis à une réglementation de plus en plus rigide. Ainsi, tout le monde n'a pas encore compris que les "dark patterns" sont réglementés par le Digital Services Act (DSA) - et les LLM peuvent en faire partie. Celui-ci interdit "les pratiques qui ont pour but ou pour effet de fausser ou d'altérer de manière significative la capacité des utilisateurs à prendre une décision ou à faire un choix autonome et éclairé" et couvre donc bien les LLM. S'y ajoutent des réglementations dans le DSA sur les produits de bots automatisés sur les plateformes en ligne, qui sont reconnus comme des risques systémiques - l'IA pouvant également être saisie et réglementée par le DSA en tant que système de recommandation. Ce domaine, jusqu'ici sous-estimé, représentera encore beaucoup de travail pour les agences et les développeurs d'IA.

Responsabilité de la direction

Les risques de responsabilité décrits ici concernent le fabricant, généralement une société, c'est-à-dire une personne morale. Il s'agit néanmoins d'un risque pour les gérants et les conseils d'administration, car ceux-ci ont l'obligation envers la société d'appliquer dans leur gestion la diligence d'un dirigeant d'entreprise prudent et consciencieux. Ceux qui y contreviennent s'exposent à un éventuel recours de la société - avec la jurisprudence moderne de la Cour fédérale de justice, l'accusation pénale de déloyauté est régulièrement en ligne de mire.

```
Dans ce contexte, la situation en matière de responsabilité va s'aggraver
de manière drastique : Avec la mise en œuvre de la directive NIS2 en
Allemagne, des mesures de sécurité clairement définies sont imposées aux
entreprises de taille moyenne. Il est également défini que la direction est
personnellement responsable des conséquences des manquements dans ce
domaine - et que la société ne peut ni renoncer à de telles exigences, dont
font partie les amendes, ni conclure un accord avec la direction !
```

Un scénario exemplaire est celui où un logiciel est développé sans accompagnement juridique et où l'on s'aperçoit seulement à la fin, peu avant le lancement sur le marché, que l'utilisation du logiciel n'est pas juridiquement possible. Dans ce cas, des actifs de la société ont été mobilisés sans que le risque ait été évalué au préalable - cela retombe sur les pieds. Et ce n'est malheureusement pas un cas particulier, de nombreuses personnes ne cherchent un conseil juridique que lorsque le logiciel est presque prêt à être commercialisé, ce qui peut entraîner des coûts supplémentaires considérables et donc des questions de responsabilité.

L'expérience montre que ce risque est considérablement sous-estimé par les gérants de sociétés unipersonnelles. Cela s'explique notamment par le fait qu'en raison de la prétendue identité de fait des personnes, on laisse les limites s'estomper et on pense que "là où il n'y a pas de juge, il n'y a pas de bourreau". Cependant, si la société devient insolvable et qu'un administrateur judiciaire prend les rênes, la première chose qu'il fera sera d'examiner et de faire valoir des droits contre la direction.

Obligation d'indemnisation des fournisseurs d'IA

Cela ne devrait pas surprendre et n'est repris ici qu'à titre de clarification : Quiconque propose une IA, qu'il s'agisse d'une solution individuelle, d'un intermédiaire de solutions standard ou d'une IA en tant que service, est responsable en cas d'erreur. Ce qui constitue une erreur doit être décidé au cas par cas. Un chatbot qui insulte les utilisateurs, donne des informations erronées ou pose des questions inadmissibles est par exemple défectueux. Les demandes de dommages et intérêts des utilisateurs envers le client devront être payées en recours, tout comme les amendes pour traitement illicite des données.

```
D'où l'avertissement urgent : il peut être tentant d'entraîner une base de
données vectorielles open source et de la proposer ensuite comme chatbot,
mais cela peut être un désastre financier. Il convient de souligner qu'en
l'état actuel de la législation, un comportement erroné d'une IA peut déjà
constituer un défaut de produit. Les fournisseurs de logiciels, tout comme
les agences de publicité, doivent notamment fournir des informations de
base sur les problèmes juridiques connus. La seule violation d'une telle
obligation d'information peut déjà déclencher des demandes de dommages et
intérêts !
```

Perspectives

Même s'il s'agit ici de montrer clairement qu'il existe déjà un scénario de responsabilité réel et à prendre au sérieux, il ne faut pas oublier d'évoquer les perspectives. Il convient de noter que la densité de la réglementation ne diminue pas - et ne fait qu'étendre le cadre juridique existant, sans le remplacer. L'AI-Act règle les questions d'admissibilité et les conditions d'exploitation d'une IA, l'instrument réglementaire étant ici les amendes.

Alors que l'AI Act est décisif pour l'évaluation de l'admissibilité d'une IA, la directive sur l'IA est beaucoup plus importante pour le sujet concerné ici : elle est moins au centre de l'attention du public, mais elle créera des facilités de preuve et des droits à la divulgation de preuves qui faciliteront considérablement la mise en œuvre des demandes de dommages et intérêts contre les exploitants de produits d'IA. En particulier, le fait de ne pas se conformer à l'ordre de divulgation des preuves

entraîne une présomption de faute dans les demandes de dommages et intérêts en cas d'utilisation de systèmes d'IA. Il s'agit là d'un instrument peu considéré qui orientera de manière décisive les litiges civils concernant les produits d'IA.

En outre, il convient de rappeler la nouvelle directive sur la responsabilité du fait des produits, qui s'appliquera aux logiciels et à l'IA. Tout comme la directive sur la responsabilité en matière d'IA, elle prévoira un droit à la divulgation des preuves et pourrait, avec l'allègement des preuves prévu par la directive sur l'IA, devenir une épée de Damoclès dans les litiges civils. Ce droit à la divulgation devrait justement mettre en évidence l'immense importance que revêtira à moyen terme une documentation juridiquement réfléchie du développement et de la formation des logiciels d'IA. Le Cyberresilienz Act et le règlement européen réformé sur la sécurité des produits ne doivent pas être sous-estimés en tant que futures lois de protection.

Conclusion et recommandation d'action

Il existe un cadre de responsabilité existant qui sera de plus en plus développé au cours des prochaines années. C'est également important, car le cadre de responsabilité existant est certes utilisable, mais aussi lacunaire - et conduira, dans la jurisprudence, à ce que des décisions judiciaires prétendument conformes aux intérêts et donc incalculables soient prises dans des cas particuliers.

C'est une grave erreur d'ignorer le régime de responsabilité existant et de se concentrer uniquement sur l'AI-Act. Il serait tout aussi fatal d'ignorer l'AI-Act uniquement parce que l'on ne sait pas encore s'il sera finalement adopté et, le cas échéant, sous quelle forme. Il devrait être clair que la préparation juridique doit commencer dès la phase de conception. Une procédure sommaire pourrait être la suivante :

1. conception : il convient de définir un domaine d'application et d'orienter l'AI-Act en fonction de ce domaine d'application clair. Le domaine d'application doit être vérifié à chaque étape de développement ; il n'y a pas de mal à ce qu'un Ki puisse couvrir différents scénarios, mais un domaine d'application clairement défini doit être classé dans l'AI-Act ;
2. **Orientation** : en cas d'utilisation dans un environnement sensible, comme en

particulier l'utilisation vis-à-vis des travailleurs ou dans le milieu médical, le développement devra être conçu différemment ; l'IA devrait être développée de manière à ce qu'une adaptation aussi dynamique que possible soit envisageable au cas par cas, afin de répondre aux conditions concrètes et aux types de données à traiter ; une IA dans un environnement sensible, dont les interventions relevant du droit de la personnalité ne peuvent pas être contrôlées au cas par cas, devrait en principe poser problème et donner lieu à des litiges juridiques ;

3. **Développement** : d'une part, une documentation continue orientée vers la directive sur l'IA devrait être installée ; d'autre part, compte tenu du régime de responsabilité établi, il devrait exister un contrôle de qualité (à nouveau documenté) en ce qui concerne le développement de logiciels et le processus d'entraînement ; une attention particulière doit être accordée à la thématique des biais, la discrimination doit jouer un rôle dès le début de l'entraînement et devrait être accompagnée par un spécialiste qui peut s'exprimer sur l'éthique ;
4. distribution__ : l'observation continue du produit doit être mise en place ; les problèmes ou les nouvelles connaissances qui apparaissent doivent être traités immédiatement et mis en œuvre par des mises à jour pendant toute la durée d'utilisation ; il est vivement recommandé de procéder à des contrôles propres et continus de son propre système, qui, en cas d'utilisation dans un environnement sensible, doivent être plus intensifs que pour des solutions standard générales ; la distribution de solutions d'IA exigera obligatoirement que l'on garde un œil sur les connaissances scientifiques et techniques actuelles et que l'on compare en permanence son propre logiciel avec celles-ci - même si aucun message d'erreur ou complication n'est encore connu ;

À propos de l'auteur et du cabinet

Auteur: Avocat Jens Ferner, spécialiste du droit de l'informatique et du droit pénal, Ferner.Legal / Ferner-Alsdorf.de

Ce bref article, qui donne un aperçu non exhaustif des thèmes liés au développement et à l'utilisation de l'IA, a été écrit dans un éditeur Markdown (d'où le design inexistant).

JF est un ancien développeur de logiciels et auteur de livres sur le langage de script PHP ; aujourd'hui, il programme en Python à titre de loisir, s'est longtemps intéressé aux réseaux neuronaux et préfère actuellement la programmation quantique au moyen de Qiskit. Sur le plan juridique, il s'occupe, outre de la défense pénale, de questions de droit technologique et de responsabilité des conseils d'administration.

Cabinet d'avocats Ferner Alsdorf (Carl-Zeiss-Strasse 5, 52477 Alsdorf, kontakt@ferner-alsdorf.de, 02404 92100, Ferner-Alsdorf.de/impressum)