... ZAOULI N°15, Septembre 2026, pp. 674-721 ISSN : 2788-9343

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

La gestion contractuelle du risque de fraude numérique en droit ivoirien : de l'efficacité du contrat à ses limites structurelles

Ladji YEO
Docteur en droit privé
Enseignant-chercheur, ESATIC
ladji.yeo@esatic.edu.ci

Résumé.
À mesure que les activités économiques, administratives et sociales se déploient sur des infrastructures interconnectées, le risque de fraude numérique cesse d'être un aléa périphérique pour devenir une donnée structurante de la relation contractuelle. En droit ivoirien, le contrat participe à la maîtrise de ce risque en traduisant les exigences légales de sécurité en stipulations de prévention, de détection, d'allocation des responsabilités, de contrôle, de notification et de réversibilité. Cette fonction permet de caractériser une gestion contractuelle du risque de fraude numérique, entendue comme l'ensemble des techniques conventionnelles par lesquelles les parties anticipent la fraude, en réduisent la probabilité ou les effets, en répartissent les conséquences et organisent la réponse à sa réalisation. L'étude montre toutefois que cette technique, bien qu'opératoire, demeure structurellement incomplète. La bilatéralité du contrat s'accorde imparfaitement avec le caractère réticulaire et potentiellement systémique du risque, tandis que les asymétries informationnelles, la dépendance technologique et les contraintes techniques peuvent réduire l'effectivité des stipulations convenues. La gestion contractuelle ne constitue dès lors pas un modèle autosuffisant de maîtrise du risque, mais une composante d'une gouvernance intégrée de la résilience numérique, articulant autonomie contractuelle, prescriptions légales, régulation institutionnelle et référentiels techniques.

Mots-clés : Gestion contractuelle ; Fraude numérique ; Cybersécurité ; Droit des contrats ; Effectivité contractuelle ; Droit ivoirien.

Abstract.
As economic, administrative, and social activities increasingly rely on interconnected infrastructures, the risk of digital fraud is no longer a peripheral concern but has become a fundamental aspect of contractual relationships. Under Ivorian law, contracts help manage this risk by translating legal security requirements into provisions regarding prevention, detection, allocation of liability, monitoring, notification, and reversibility. This function enables the characterization of a contractual approach to managing the risk of digital fraud, understood as the set of contractual techniques through which the parties anticipate fraud, reduce its probability or effects, allocate its consequences, and organize the response to its occurrence. The study shows, however, that this approach, while effective, remains structurally incomplete. The bilateral nature of the contract is imperfectly aligned with the networked and potentially systemic nature of the risk, while information asymmetries, technological dependence, and technical constraints can reduce the effectiveness of the agreed-upon provisions. Contractual management is therefore not a self-sufficient model for risk control, but rather a component of integrated governance of digital resilience, linking contractual autonomy, legal requirements, institutional regulation, and technical standards.

Keywords: Contractual management; Digital fraud; Cybersecurity; Contract law; Contractual effectiveness; Ivorian law.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

Introduction

Le contrat est traditionnellement présenté comme un instrument de prévision. En fixant à l'avance les obligations des parties et les conséquences de leur inexécution, il soustrait l'échange à une part d'incertitude et permet aux opérateurs d'ordonner juridiquement l'avenir. (BERGEL, J.-L., 2008, pp. 273-274) Cette fonction classique acquiert une importance particulière dans l'environnement numérique. La dématérialisation des échanges, l'interconnexion des systèmes, la circulation massive des données, l'externalisation des ressources informatiques et la dépendance à l'égard d'infrastructures numériques exposent en effet les relations contractuelles à des formes renouvelées de risque frauduleux. La fraude en elle-même et quelle que soit la discipline du droit, est constituée d'agissements illicites par emploi de moyens légaux ou irréguliers (YEO, L., 2018, p. 7). Elle designe un « acte qui a été réalisé en utilisant des moyens déloyaux destinés à surprendre un consentement, à obtenir un avantage matériel ou moral indu ou réalisé avec l'intention d'échapper à l'exécution des lois »[1]. Elle n'est donc pas née avec le numérique. Par exemple, l'usurpation d'identité, la falsification, la tromperie ou le détournement ont toujours été susceptibles d'affecter la formation ou l'exécution des contrats indépendamment de leur forme numérique. Par conséquent, le numérique n'en modifie pas nécessairement la nature juridique. Toutefois, il en

[1]Voir le terme « fraude » in BRAUDO (B.), Dictionnaire du droit privé, 1996-2016, en ligne : http://www.dictionnaire-juridique.com/definition/fraude.php (consulté le 10 juillet 2026).

transforme les conditions de réalisation, l'échelle, la vitesse de propagation, les possibilités de détection ainsi que les modalités de prévention et de traitement. C'est en ce sens que peut être identifié un risque de fraude numérique, dont la maîtrise devient une préoccupation croissante des relations contractuelles. (BILE-AKA, J., 2010, p.2)

Le risque ici, est un « évenement éventuel, incertain, dont la réalisation ne dépend pas exclusivement de la volonté des parties et pouvant causer un dommage » (GUINCHARD (S.) et DEBARD (T.), 2014, 983 p., p. 839). Il fait donc référence à la possibilité de réalisation d'un événement incertain susceptible de produire des conséquences préjudiciables. ([1]ÇELEBİ (Ö.), 2020, p. 57-106, spéc. p. 59) Rapportée à la fraude, cette notion conduit moins à rechercher l'existence d'une catégorie nouvelle de comportement frauduleux qu'à s'intéresser aux circonstances particulières dans lesquelles celui-ci est susceptible de survenir. Le risque de fraude numérique peut ainsi être entendu comme l'éventualité qu'un comportement frauduleux affecte la formation, l'exécution ou l'extinction d'une relation contractuelle en exploitant, directement ou indirectement, les technologies, systèmes, données, procédés d'identification, d'authentification, de communication ou de paiement propres à l'environnement numérique. Il peut notamment se matérialiser par l'usurpation d'identité numérique, l'hameçonnage, la compromission de messageries professionnelles, les fraudes aux moyens de paiement, la manipulation de données ou encore l'atteinte à l'intégrité d'un système d'information en vue d'obtenir un avantage illégitime.

Ainsi entendu, le caractère numérique du risque ne résulte pas de la seule dématérialisation du contrat. Un contrat

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

conclu électroniquement peut être affecté par une fraude dont le procédé ne présente aucune spécificité numérique ; inversement, un contrat initialement conclu hors ligne peut être exposé, au cours de son exécution, à une fraude reposant sur la compromission d'un système, d'une identité ou d'un moyen de paiement numérique. La qualification tient donc moins au support du contrat qu'au rôle joué par l'environnement numérique dans l'apparition, la réalisation, la propagation ou le traitement du risque frauduleux. Sa singularité est, en ce sens, principalement fonctionnelle. La distance entre les acteurs, l'automatisation de certaines opérations, la massification potentielle des atteintes et l'interdépendance des systèmes peuvent accroître l'exposition au risque et en amplifier les conséquences. Un incident initialement localisé est ainsi susceptible, par le jeu des interdépendances techniques et contractuelles, d'affecter une chaîne de fournisseurs, de sous-traitants et d'utilisateurs. Le risque de fraude numérique présente dès lors des dimensions simultanément technique, économique et juridique.

Cette reconfiguration du risque conduit à déplacer l'analyse de la seule réaction à la fraude vers son anticipation. La question n'est plus seulement de déterminer les sanctions applicables ou les conditions de réparation du dommage après sa réalisation. Elle consiste également à rechercher comment les acteurs peuvent, en amont, prévenir la fraude, en réduire la probabilité ou les conséquences et organiser la réponse à sa survenance. C'est dans cette perspective que la notion de gestion contractuelle du risque mérite d'être mobilisée.

D'inspiration notamment anglo-saxonne et courante dans le vocabulaire de la gestion des risques, cette notion n'est pas, en tant que telle, consacrée comme catégorie générale par le droit positif ivoirien. Son intérêt doctrinal réside précisément dans sa capacité à fédérer des mécanismes juridiques dispersés. La gestion du risque ne se confond ni avec la seule prévention, qui tend à éviter sa réalisation, ni avec la réparation, qui intervient après le dommage. Elle désigne plus largement un processus de maîtrise consistant à identifier et évaluer le risque, à réduire sa probabilité ou ses effets, à transférer ou répartir certaines de ses conséquences et à préparer la réponse à l'incident.[2]

Transposée au contrat, la gestion contractuelle du risque de fraude numérique peut alors être définie comme l'ensemble des mécanismes conventionnels par lesquels les parties anticipent le risque frauduleux lié à l'environnement numérique, en préviennent ou en réduisent la réalisation et les effets, en répartissent les conséquences et organisent la réponse à sa survenance. Cette notion permet de relire sous un angle unitaire des clauses que la pratique traite souvent séparément[3]. Leur dénominateur commun est de faire du contrat non plus seulement le support d'un échange, mais

[2]La gestion des risques permet en effet, de remplacer une perception diffuse des vulnérabilités par une connaissance rationnelle. Elle permet d'optimiser le traitement des risques grâce à un programme global et cohérent, mettant en oeuvre une palette d'outils, en particulier des outils de financement et de réduction des risques non matériels. *Cf.* BARTHÉLEMY (B.) et COURRÈGES (Ph.), Gestion des risques. Méthode d'optimisation globale, 2e éd., Éditions d'Organisation / Eyrolles, 2004, p. 34

[3]Ce sont : les clauses de sécurité des systèmes d'information, obligations de conformité et de loyauté, engagements de niveau de service, plans de continuité et de reprise d'activité, procédures de notification d'incident, droits d'audit, garanties, clauses de responsabilité, assurances, obligations de sauvegarde, de portabilité ou encore de réversibilité.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

également un instrument d'organisation anticipée de l'incertitude frauduleuse.[4]

L'intérêt d'une telle lecture est particulièrement marqué en droit ivoirien. Le législateur a pris certaines dispositions à propos lorsque le numérique s'invique dans le contrat. Il s'agit notamment des exigences de sécurité imposées par la loi relative à la protection des données à caractère personnel[5] et celle des transactions électroniques[6], de la pénalisation des diverses atteintes aux systèmes d'information et aux données[7] puis, des exigences relatives à la sécurité et à la continuité des réseaux et services[8]. À ces textes, s'ajoutent les référentiels de sécurité des systèmes d'information et l'architecture institutionnelle ivoirienne de cybersécurité. Dans cet environnement normatif, le contrat peut constituer un lieu de concrétisation de prescriptions légales et réglementaires qui, pour devenir pleinement opérationnelles dans les rapports entre acteurs, appellent leur traduction en obligations précises, mesurables et contrôlables.

L'intérêt théorique du sujet apparaît alors dans le changement de perspective qu'il propose. Il ne s'agit pas d'ériger la fraude numérique en une catégorie juridique nécessairement autonome par rapport aux mécanismes frauduleux traditionnels. Il s'agit plutôt de montrer que la

[4]Le risque sert à légitimer l'existence des règles juridiques et donc sert de base au contrat. V. TRUDEL (P.), « Le risque, fondement et facteur d'effectivité du droit », p. 256.
[5]Cf. la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.
[6]Cf. la loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques.
[7]Cf. la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.
[8]Cf. la loi n° 2024-325 du 6 juin 2024 relative aux communications électroniques.

transformation des conditions de réalisation du risque frauduleux sous l'effet du numérique peut justifier une adaptation des techniques de sa maîtrise contractuelle. L'intérêt pratique est tout aussi manifeste : face à un risque susceptible d'affecter l'identité des cocontractants, l'intégrité des données, la sécurité des paiements, la continuité des prestations ou encore la responsabilité des différents intervenants, la qualité de l'anticipation contractuelle peut conditionner l'efficacité de la prévention comme celle de la réaction à l'incident.

Pour autant, reconnaître l'utilité du contrat ne signifie pas lui attribuer une puissance qu'il ne possède pas. La technique contractuelle demeure structurée par le principe de relativité et par l'identification de parties déterminées. Or le risque de fraude numérique se développe dans des écosystèmes où l'intervention, la défaillance ou la complicité d'un tiers peut compromettre l'exécution de contrats auxquels celui-ci n'est pas partie. La causalité peut être distribuée entre plusieurs intervenants et la vulnérabilité d'un fournisseur produire des effets en cascade sur l'ensemble d'une chaîne contractuelle. À cette difficulté structurelle s'ajoute une difficulté d'effectivité : le contrat ne produit pleinement son effet préventif que si les parties disposent de l'information, du pouvoir de négociation, des compétences techniques et des moyens matériels nécessaires à la mise en œuvre des obligations stipulées.

Dès lors, la question centrale est la suivante : dans quelle mesure le contrat constitue-t-il, en droit ivoirien, un instrument juridiquement efficace de gestion du risque de fraude numérique alors que les caractéristiques systémiques, évolutives et interconnectées de ce risque tendent à dépasser les capacités du modèle contractuel classique ? L'hypothèse

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

défendue est que le contrat constitue un instrument opératoire de première importance, sans pouvoir former un dispositif autosuffisant. Son efficacité tient à sa capacité à traduire l'anticipation du risque en obligations de prévention, de détection, de coopération, de répartition et de réaction. Ses limites commandent toutefois son articulation avec les normes impératives, la régulation, les standards techniques et une gouvernance plus largement écosystémique.

L'étude se situe ainsi à la croisée du droit des obligations et du droit du numérique. Elle mobilise les catégories classiques du droit des contrats tout en les confrontant aux transformations du risque frauduleux induites par les usages numériques. Elle s'appuie principalement sur le droit ivoirien en vigueur, éclairé, lorsque cela est utile, par la doctrine et les expériences comparées ainsi que par les référentiels techniques susceptibles d'influencer la pratique contractuelle. Il ne s'agit donc pas de dresser un catalogue exhaustif de clauses ni d'élaborer une théorie générale de la fraude numérique, mais d'identifier la logique juridique qui sous-tend la gestion contractuelle de ce risque et d'en apprécier la portée.

La démonstration conduit ainsi à envisager, d'abord, l'affirmation de la gestion contractuelle comme instrument de maîtrise du risque de fraude numérique, avant de mettre en évidence les limites de cette gestion face aux caractéristiques contemporaines du risque de fraude numérique.

I. L'affirmation de la gestion contractuelle comme instrument de maîtrise du risque de fraude numérique

La gestion contractuelle du risque de fraude repose sur une idée simple. Le risque n'est pas extérieur au contrat. Il peut en

devenir un objet. Les parties peuvent identifier les événements frauduleux redoutés. Elles peuvent définir les comportements attendus avant et pendant l'incident. Elles peuvent organiser les conséquences de sa réalisation. Le contrat exerce ainsi une fonction préventive et allocative.[9] Cette fonction se prolonge, dans les opérations numériques, par une densification des obligations de sécurité et de détection de la fraude. L'efficacité de cette technique tient, d'une part, à la contractualisation de la prévention du risque de fraude numérique et, d'autre part, à la contractualisation de sa répartition et de son traitement.

1.1. La contractualisation de la prévention du risque de fraude numérique

Prévenir contractuellement le risque de fraude numérique consiste à transformer une menace abstraite en obligations juridiquement déterminées. L'opération suppose, en premier lieu, d'identifier et de formaliser les risques de fraude auxquels les parties sont exposées. Elle implique, en second lieu, de traduire cette analyse en obligations positives de sécurité, de détection et de continuité dont l'exécution peut être contrôlée.

[9]En réalité dans le contrat, les clauses de sécurité, d'audit, de notification, de pénalités ou de responsabilité jouent le même rôle que « la règle » selon Trudel. Selon lui en effet, l'effectivité d'une norme dépend de sa capacité à générer, chez les sujets, une perception significative de risque attachée à sa transgression. Transposée au contrat, cette analyse éclaire la fonction préventive des stipulations de sécurité : elles n'organisent pas seulement des diligences techniques ; elles rendent opposables des conséquences (responsabilité, pénalités, résiliation). *Cf.* TRUDEL (P.), « Le risque, fondement et facteur d'effectivité du droit », p. 261.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

1.1.1. L'identification et l'anticipation conventionnelles des risques de fraude

L'anticipation constitue le premier ressort de la gestion contractuelle du risque de fraude. Avant même la survenance d'un incident, le contrat permet aux parties d'identifier les menaces susceptibles d'affecter l'opération et d'organiser les réponses qui leur seront apportées. Cette démarche est particulièrement importante dans les contrats d'hébergement, de cloud computing, de maintenance informatique, d'infogérance, de fourniture de services de paiement ou de communications électroniques. Dans ces opérations, la pertinence du dispositif contractuel dépend de l'identification préalable des actifs critiques, des vecteurs de fraude, des vulnérabilités, des dépendances techniques ainsi que des conséquences potentielles d'un incident. Une clause de sécurité ne présente, en effet, de véritable portée que si elle correspond aux risques propres à l'opération et si les obligations qu'elle établit sont suffisamment précises pour permettre d'en apprécier l'exécution.

L'identification des risques constitue ainsi le préalable à leur traduction en obligations contractuelles. Elle peut notamment se matérialiser par une cartographie des risques annexée au contrat, une matrice de responsabilité, un questionnaire de sécurité précontractuel, des exigences de conformité ou encore des procédures de gestion des incidents. Les réponses fournies par le prestataire lors de la phase précontractuelle peuvent elles-mêmes être contractualisées et devenir de véritables engagements. De même, celui-ci peut être tenu de communiquer une documentation relative à son architecture technique, aux dispositifs de prévention de la fraude ou aux procédures

destinées à assurer la continuité du service. Ces instruments permettent de dépasser une formulation générique par laquelle le prestataire s'engagerait simplement à assurer la « sécurité » du service. Le contrat peut alors déterminer les actifs concernés, leur niveau de criticité, les mesures minimales de prévention, les mécanismes de détection, les délais de réaction, les circuits d'alerte, les responsabilités respectives des parties et les modalités de preuve de l'exécution des obligations. L'identification du risque permet ainsi de transformer une obligation abstraite de sécurité en obligations opérationnelles susceptibles d'être contrôlées.

En droit ivoirien, cette fonction anticipatrice du contrat s'inscrit dans un environnement normatif qui impose déjà certaines exigences de sécurité. La loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel met notamment à la charge du responsable du traitement des obligations destinées à assurer la sécurité des données[10]. La législation relative aux communications électroniques comporte également des prescriptions intéressant la sécurité, l'intégrité et la continuité des réseaux et services[11]. Quant à la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité, l'incrimination de diverses atteintes commises au moyen des systèmes d'information contribue à identifier des comportements contre lesquels les acteurs économiques doivent se prémunir. Le contrat ne crée donc pas nécessairement l'obligation de sécurité ; il en assure souvent la concrétisation. Il traduit les exigences légales en

[10]Les obligations du responsable du traitement et de ses subordonnés sont notamment précisées aux articles 39 à 45 de la loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

[11]V. Le législateur encadre la sécurité des réseaux et des services, la confidentialité des communications et l'identification des utilisateurs. Cf., loi N°2024-352 du 6 juin 2024 relative aux transactions électrnoniques : art 97 à 105.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

obligations adaptées à l'opération considérée en précisant qui doit intervenir, selon quelles modalités, dans quels délais et sous quel contrôle.

Les référentiels techniques peuvent compléter cette opération de spécification. Le NIST Cybersecurity Framework 2.0 structure ainsi la gestion du risque autour de six fonctions : Govern, Identify, Protect, Detect, Respond et Recover.[12] De même, les travaux de l'ENISA consacrés au paysage des menaces, à la réponse aux incidents ou à la continuité fournissent des éléments susceptibles d'orienter la détermination des mesures de sécurité. Sans acquérir, par leur seule existence, la valeur de normes impératives en droit ivoirien, ces référentiels peuvent être incorporés au contrat, servir d'étalons de diligence ou inspirer la rédaction des annexes techniques. Leur intérêt juridique se manifeste alors lorsqu'ils cessent d'être de simples recommandations externes pour devenir, par le jeu de l'autonomie de la volonté, des références conventionnelles permettant d'apprécier l'exécution des obligations de sécurité.

L'anticipation contractuelle ne saurait toutefois conduire à figer les risques et les mesures destinées à les prévenir. La fraude numérique présente, par nature, un caractère évolutif. Les techniques d'ingénierie sociale se renouvellent, de nouvelles vulnérabilités logicielles apparaissent et les dépendances à l'égard de prestataires cloud, de bibliothèques open source ou de fournisseurs tiers peuvent créer de nouveaux points de défaillance. Une cartographie

[12]NIST, The NIST Cybersecurity Framework (CSF) 2.0, NIST CSWP 29, 26 février 2024.

contractuelle fondée sur une liste close de menaces risque donc de perdre progressivement sa pertinence.

Cette évolution impose de concevoir l'anticipation comme un processus dynamique plutôt que comme une opération réalisée une fois pour toutes lors de la conclusion du contrat. Les parties peuvent ainsi prévoir des obligations de veille, des audits périodiques, une réévaluation régulière des risques, ainsi que des mécanismes de révision ou de mise à jour des annexes de sécurité. Une telle démarche permet d'adapter les obligations contractuelles à l'évolution des techniques de fraude sans remettre systématiquement en cause l'économie générale du contrat.

Cette adaptabilité doit néanmoins être conciliée avec l'exigence de clarté et de sécurité juridique.[13] Une référence trop générale à un standard évolutif peut rendre incertain le contenu de l'obligation lorsque le contrat ne précise ni la version applicable ni les conditions de son actualisation. À l'inverse, la fixation excessivement détaillée et intangible des mesures de sécurité risque de rendre rapidement le dispositif contractuel obsolète. L'anticipation conventionnelle du risque se situe ainsi au point d'équilibre entre deux exigences : la précision nécessaire à l'opposabilité de l'obligation et la souplesse indispensable à son adaptation. Les clauses de révision, les mécanismes d'audit et les procédures d'actualisation des annexes permettent précisément d'organiser cet équilibre.

[13]En réalité, le traitement de l'insécurité que l'on constate trop souvent dans les divers systèmes juridiques suppose d'améliorer l'accessibilité matérielle et intellectuelle du droit pour tous et de consacrer un principe général de sécurité juridique. *Cf,* BERGEL (J.-L.), « La sécurité juridique », Revue du notariat, vol. 110, n° 2, septembre 2008, pp. 277.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

1.1.2. La formalisation des obligations de sécurité, de détection et de continuité

L'identification préalable des risques de fraude ne présente d'utilité que si elle se prolonge par la détermination d'obligations suffisamment précises pour en assurer la prévention, la détection et le traitement. La contractualisation permet précisément d'opérer ce passage de la connaissance du risque à l'organisation des comportements destinés à le maîtriser. Les contrats numériques comportent ainsi des stipulations relatives au contrôle des accès, au chiffrement, à la journalisation, aux sauvegardes, à la gestion des vulnérabilités, aux mises à jour, à la détection des anomalies ou encore à la notification des incidents de fraude. La sécurité contractuelle acquiert alors un contenu concret : elle ne désigne plus seulement une finalité à atteindre, mais un ensemble de diligences et de prestations dont l'exécution peut être appréciée.

Cette formalisation suppose, d'abord de déterminer avec suffisamment de précision la nature et l'intensité des obligations mises à la charge des parties. La distinction entre obligation de moyens et obligation de résultat conserve, à cet égard, toute son utilité. Certaines prestations peuvent être formulées sous la forme d'un résultat objectivement vérifiable. Il peut en aller ainsi du respect d'un taux de disponibilité déterminé, de la réalisation d'une sauvegarde selon une périodicité convenue ou encore de la notification d'un incident de fraude dans un délai fixé. D'autres obligations se prêtent moins à la garantie d'un résultat absolu. La prévention de toute intrusion ou de toute fraude, compte tenu de l'évolution constante des menaces, relève davantage

d'une obligation de moyens, éventuellement renforcée, imposant au prestataire de mettre en œuvre les diligences convenues au regard de l'état de l'art, de la nature du service et des risques identifiés. Cette qualification n'est pas purement théorique : elle influence directement l'appréciation de l'inexécution et, en définitive, les conditions de mise en œuvre de la responsabilité.[14]Les engagements de niveau de service, ou Service Level Agreements (SLA), participent précisément de cette objectivation des obligations. Le taux de disponibilité, le temps maximal d'interruption, le délai de prise en charge d'un incident, le délai de notification d'une fraude ou encore le délai de rétablissement du service peuvent être exprimés au moyen d'indicateurs chiffrés. La sécurité cesse ainsi d'être appréhendée exclusivement à travers des formulations générales pour devenir, sur certains aspects, une prestation mesurable. Les pénalités de service susceptibles d'accompagner ces engagements renforcent leur effectivité. Elles doivent toutefois être distinguées des mécanismes de réparation du préjudice : la compensation forfaitaire attachée au non-respect d'un niveau de service ne saurait, par elle-même, régler l'ensemble des conséquences dommageables susceptibles de résulter d'une fraude numérique.

Ensuite, la formalisation des obligations doit intégrer la continuité et la reprise de l'activité. La sécurité ne consiste pas seulement à empêcher la réalisation du risque ; elle suppose également d'organiser les conditions dans lesquelles l'activité

[14]En matière de traitement de données à caractère personnel, le ligislateur oblige la personne en charge du traitement (le responsable ou son sous-traitant) à assurer la sécurité des données et à être tenu pour responsable dans le cas échéant. *Cf*. Loi loi N° 2013-450 du 19 juin 2013, relative à la protection des données à caractère personnel, art. 19, 20 al.1 et 41.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

pourra être maintenue ou rétablie lorsqu'un incident survient. Les plans de continuité d'activité et les plans de reprise d'activité, lorsqu'ils sont intégrés ou annexés au contrat, permettent de déterminer les procédures de sauvegarde, les mécanismes de redondance, les sites de secours, la priorisation des fonctions critiques ainsi que les objectifs de temps et de point de reprise.[15]

Le droit ivoirien offre un cadre propice à cette contractualisation. Lorsque la législation impose des obligations de sécurité, notamment en matière de traitement de données à caractère personnel ou de communications électroniques, le contrat peut en préciser les modalités concrètes d'exécution. Il ne se substitue pas aux prescriptions impératives. Il les traduit dans l'économie particulière de l'opération et peut, lorsque cela est juridiquement possible, renforcer le niveau de protection qu'elles établissent. La norme légale fixe ainsi le cadre auquel les parties sont tenues, tandis que la norme contractuelle adapte les obligations aux caractéristiques techniques et aux risques propres à la relation considérée.

Enfin, la précision des obligations serait cependant insuffisante si leur créancier ne disposait d'aucun moyen d'en contrôler l'exécution et d'en rapporter la preuve. Le droit d'audit occupe, de ce point de vue, une place essentielle. Une obligation de sécurité dont l'exécution échappe à toute possibilité de vérification risque de conserver une portée

[15]Cela doit être tout comme il en serait dans un manuel de gestion de crise. Il s'agit ainsi de définir des objectifs à court terme, précis et spécifiques, et non pas des objectifs globaux tels que « assurer la survie de l'entreprise » ou « limiter les dégâts causés par le sinistre ». Ce sera par exemple « éviter la propagation au local voisin » ou « diffuser une information unique aux médias ». *Cf.* BARTHÉLEMY (B.) et COURRÈGES (Ph.), op. cit., p. 95.

largement déclaratoire. L'audit, la remise périodique de rapports, la communication de certifications ou encore la réalisation de tests de sécurité encadrés permettent de réduire l'asymétrie informationnelle existant notamment entre le prestataire, qui maîtrise son infrastructure, et le client qui lui confie certaines opérations.

L'efficacité de ces mécanismes dépend toutefois de leur degré de précision. Le contrat doit notamment déterminer la fréquence des audits, leur périmètre, les conditions de préavis, les obligations de confidentialité, la répartition des coûts, les modalités d'accès aux informations pertinentes ou aux sous-traitants ainsi que les conséquences attachées aux non-conformités constatées. Il peut également prévoir un délai de remédiation et organiser un contrôle ultérieur de la correction des insuffisances relevées. La prévention contractuelle devient alors une ingénierie du contrôle autant qu'une ingénierie de l'obligation.

Cette logique de contrôle se prolonge naturellement sur le terrain probatoire. La fraude numérique laisse généralement des traces dont l'exploitation peut être déterminante pour établir la chronologie des faits, identifier une défaillance ou, au contraire, démontrer l'exécution des diligences convenues. Les journaux d'événements, les rapports d'audit et de tests, les certificats de conformité, les historiques d'accès ainsi que les traces de notification constituent autant d'éléments susceptibles d'être mobilisés. Le contrat peut en organiser la génération, la conservation, l'intégrité, l'accessibilité et les conditions de communication. Il contribue ainsi à la sécurité juridique de la relation en préparant, dès la conclusion du contrat, les éléments susceptibles d'éclairer ultérieurement l'appréciation de son exécution.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

Par ailleurs, la formalisation contractuelle doit tenir compte du caractère nécessairement coopératif de la lutte contre la fraude numérique. La sécurité d'une opération ne dépend généralement pas du comportement d'un seul cocontractant. Le client peut être tenu de configurer correctement ses accès, de protéger ses moyens d'authentification, de former ses utilisateurs, de signaler les anomalies ou de respecter certaines procédures internes. Le prestataire doit, pour sa part, mettre en œuvre les dispositifs de sécurité convenus, fournir les informations nécessaires et réagir aux alertes dans les délais prévus. Le contrat peut organiser cette coopération au moyen de procédures de signalement, de canaux de communication dédiés, de mécanismes d'escalade et de délais de réponse.

1.2. La contractualisation de la répartition et du traitement du risque de fraude numérique

La gestion contractuelle du risque de fraude ne saurait se limiter à sa prévention. Quelle que soit la qualité des mesures de sécurité mises en œuvre, la survenance d'un incident ne peut être totalement exclue. Le contrat doit donc envisager l'hypothèse dans laquelle le risque se réalise et déterminer les conséquences qui en découlent pour les parties. Cette fonction intervient à deux niveaux complémentaires. Il s'agit, d'une part, de déterminer qui supportera les responsabilités et les coûts résultant de la fraude (1) et, d'autre part, d'organiser la réponse à l'incident, la restauration de l'activité et, lorsque la poursuite de la relation devient impossible, les conditions de sortie de crise (2).

1.2.1. L'allocation conventionnelle des responsabilités et des coûts du risque de fraude

L'allocation du risque constitue une fonction classique du contrat. Dans les relations numériques, elle revêt cependant une technicité particulière en raison de la pluralité des causes susceptibles de concourir à la réalisation d'une fraude. Celle-ci peut résulter d'une défaillance de l'infrastructure du prestataire, d'une mauvaise configuration imputable au client, d'une compromission des identifiants, d'un comportement fautif d'un utilisateur, de l'intervention d'un sous-traitant ou encore de l'action d'un tiers malveillant. La détermination conventionnelle des responsabilités suppose donc, en premier lieu, de rattacher chaque risque à la sphère de maîtrise de l'acteur qui paraît le mieux placé pour le prévenir ou en limiter les conséquences.

Cette approche trouve un éclairage dans l'analyse économique du droit et, notamment, dans les travaux de Guido Calabresi relatifs au coût des accidents. (CALABRESI (G.), 1970. pp. 410-411) L'une des questions centrales consiste à rechercher l'acteur susceptible de prévenir le dommage au moindre coût ou de supporter et répartir plus efficacement ses conséquences économiques. Transposée au risque numérique, cette logique invite à dépasser une répartition uniforme des responsabilités pour tenir compte de la maîtrise effective des différents facteurs de risque. Le contrat peut ainsi distinguer les risques liés à l'infrastructure du prestataire, ceux qui relèvent de la configuration des systèmes du client, ceux qui résultent de la gestion des identifiants et des terminaux, ou encore ceux qui trouvent leur origine dans l'intervention de tiers.

Cette allocation peut être complétée par des clauses de garantie, d'indemnisation, d'exclusion de certaines catégories

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

de préjudices ou de plafonnement de responsabilité. Ces stipulations permettent aux parties de déterminer, en amont, l'étendue de la charge économique susceptible de résulter de la fraude. Les plafonds de responsabilité peuvent notamment être modulés en fonction de la criticité de la prestation, de la nature des données concernées ou encore du niveau de risque accepté. Cette modulation présente une cohérence particulière lorsque certaines opérations exposent les parties à des conséquences financières sans commune mesure avec le prix ordinaire du service.

La liberté contractuelle rencontre toutefois ici ses limites juridiques. L'allocation conventionnelle du risque ne signifie ni disparition de l'obligation ni éviction des normes impératives. Une clause organisant les conséquences financières d'un manquement ne saurait, par sa seule existence, faire disparaître les obligations que la loi impose à une partie. Les prescriptions résultant notamment de la législation ivoirienne relative à la protection des données à caractère personnel demeurent applicables lorsqu'elles présentent un caractère impératif. De même, la loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité incrimine différents comportements portant atteinte aux systèmes d'information ou mettant en œuvre certains procédés frauduleux. Les conséquences pénales attachées à de tels comportements échappent à la volonté des cocontractants.

Il importe donc de distinguer le transfert conventionnel des conséquences économiques du risque de la suppression de l'obligation dont la violation a contribué à sa réalisation. Une clause limitative peut encadrer les conséquences financières d'un manquement dans les limites admises par le

droit applicable ; elle ne transforme pas, pour autant, une obligation contractuellement ou légalement imposée en simple faculté. La cohérence du dispositif suppose ainsi de mettre en relation l'étendue de la responsabilité, la criticité de la prestation, la gravité potentielle de la fraude, le prix du service et la capacité respective des parties à prévenir ou à assurer le risque. Un plafonnement uniforme et déconnecté de ces éléments pourrait réduire considérablement la fonction préventive recherchée par la contractualisation.

L'allocation du risque remplit en effet une fonction incitative. La partie qui sait qu'elle supportera tout ou partie des conséquences économiques d'une défaillance relevant de sa sphère de maîtrise est incitée à investir dans sa prévention. À l'inverse, une dissociation excessive entre la maîtrise du risque et la charge de ses conséquences peut affaiblir cette incitation. L'efficacité du contrat dépend donc non seulement de la précision avec laquelle les responsabilités sont réparties, mais également de la cohérence existant entre le pouvoir de prévenir le risque et l'exposition aux conséquences de sa réalisation.

Cette allocation conventionnelle peut être complétée par un transfert assurantiel. L'assurance cyber ne fait pas disparaître le risque de fraude ; elle permet d'en transférer certaines conséquences financières à un tiers assureur. Elle peut notamment contribuer à absorber des coûts liés à la gestion de crise, à la restauration des systèmes, à certaines pertes d'exploitation ou à la mise en jeu de responsabilités, selon l'étendue exacte des garanties souscrites. Articulée aux mécanismes contractuels de prévention et de responsabilité, elle participe ainsi à la résilience économique de l'organisation.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

L'assurance ne saurait toutefois constituer un substitut aux obligations de sécurité. L'étendue de la couverture dépend des garanties effectivement souscrites, mais également des exclusions, franchises, plafonds, obligations déclaratives et autres conditions prévues par la police. La coordination entre le contrat de service numérique et le contrat d'assurance revêt dès lors une importance particulière. Le premier peut imposer à un prestataire le maintien d'une couverture déterminée, la justification périodique de celle-ci ou l'information du cocontractant en cas de modification substantielle. Une telle articulation permet de réduire le risque qu'un transfert contractuel de responsabilité ne corresponde, en pratique, à aucune capacité financière suffisante pour en supporter les conséquences.[16]

L'allocation conventionnelle doit également prendre en considération la dimension internationale des opérations numériques. Les infrastructures peuvent être réparties entre plusieurs États, les données circuler entre différentes juridictions et les prestataires ou sous-traitants être établis à l'étranger. La détermination du droit applicable et de la juridiction compétente participe alors à la prévisibilité du traitement juridique du risque. Ces stipulations ne permettent cependant pas nécessairement d'écarter les normes impératives susceptibles de trouver application indépendamment du choix effectué par les parties. La répartition conventionnelle du risque doit donc être pensée en articulation avec les règles de droit international privé applicables à l'opération.

[16]ÇELEBİ (Ö.), art. préc., p. 59-60.

1.2.2. L'organisation conventionnelle de la réponse, de la réversibilité et de la sortie de crise

La réalisation du risque de fraude ouvre une nouvelle séquence de la gestion contractuelle : celle du traitement de l'incident. Après avoir organisé la prévention du risque et la répartition de ses conséquences, le contrat doit déterminer les comportements attendus lorsque la fraude survient effectivement. Il contribue ainsi à réduire l'incertitude inhérente à la crise en organisant par anticipation la réaction des parties. Cette organisation conventionnelle s'articule autour de trois exigences complémentaires : l'alerte et la coordination de la réponse, le rétablissement de l'activité et, lorsque la poursuite de la relation est compromise, la réversibilité et la sortie de crise.

En premier lieu, le contrat organise la réponse immédiate à la fraude en structurant l'alerte et la coordination des interventions. Indépendamment des notifications imposées par la législation applicable, il peut obliger une partie à informer son cocontractant de la survenance ou de la suspicion d'une fraude dans un délai déterminé. Cette stipulation permet à celui-ci de prendre rapidement les mesures nécessaires à la protection de ses systèmes, de ses données ou de ses utilisateurs. Il est vrai que la planification du processus contractuel est toujours caractérisée par un certain degré d'incertitude quant à la réalisation des faits planifiés (PICHONNAZ P., 1997). Mais son efficacité suppose et réside en sa capacité à produire une définition précise du fait générateur, du délai et du contenu de l'alerte. Un seuil trop élevé risque de retarder la réaction, tandis qu'une obligation trop extensive peut multiplier les signalements peu pertinents. L'information transmise doit donc être suffisamment précoce et exploitable puis préciser, lorsque ces

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

éléments sont disponibles, la nature de l'incident, les systèmes affectés, les données éventuellement compromises et les premières mesures de confinement. Au-delà de l'alerte, le contrat peut identifier les interlocuteurs habilités, organiser les circuits d'escalade, prévoir l'activation d'une cellule de crise et répartir les tâches relatives aux investigations, à la conservation des éléments techniques et aux communications requises. Il réduit ainsi l'incertitude décisionnelle en déterminant à l'avance qui doit intervenir et selon quelles modalités. Toutefois, la maîtrise immédiate de l'incident ne suffit pas : elle doit être prolongée par le rétablissement de l'activité affectée.

En deuxième lieu, le contrat organise la restauration des systèmes et la reprise de l'activité. Une fraude numérique peut entraîner l'indisponibilité de services, l'altération de données, la suspension d'accès ou l'interruption de fonctions critiques. Les parties peuvent dès lors prévoir les conditions de restauration des systèmes, de récupération des données, de rétablissement des accès et de remise en service des fonctions essentielles. Les mécanismes de continuité et de reprise préparés en amont trouvent ici leur mise en œuvre concrète, notamment à travers la mobilisation des sauvegardes, les procédures de restauration et les délais de reprise. Le contrat assure ainsi la continuité entre la prévention et la gestion effective de la crise : les dispositifs conventionnels préalablement définis deviennent les instruments de la résilience de la relation lorsque le risque se réalise. Cependant, le rétablissement de l'activité auprès du même prestataire n'est pas toujours possible ou souhaitable. Lorsque la fraude compromet durablement la confiance ou

révèle une défaillance grave, la gestion de crise doit également préparer la sortie de la relation contractuelle.

En troisième lieu, le contrat organise la réversibilité et, le cas échéant, le transfert de l'activité. La réversibilité permet au client de récupérer les données, configurations, documentations et autres éléments nécessaires à la poursuite de son activité afin de les transférer vers un autre prestataire ou de réinternaliser la prestation. Elle présente également une fonction préventive en limitant les situations de dépendance et de verrouillage technologique susceptibles de rendre matériellement inefficace la faculté juridique de résilier le contrat. Son effectivité exige néanmoins davantage que l'affirmation de son principe. La clause doit préciser les éléments concernés, leurs formats de restitution, les délais, les coûts éventuels, l'assistance due par le prestataire, les modalités de migration ainsi que les conditions de conservation et de suppression des copies résiduelles. Pour les prestations critiques, des tests périodiques peuvent également permettre de vérifier que la réversibilité demeure techniquement réalisable. Ainsi organisée, celle-ci complète le dispositif conventionnel en permettant non seulement de répondre à la fraude et d'en surmonter les conséquences, mais aussi de quitter effectivement une relation devenue insoutenable. Cette capacité révèle cependant, dans le même temps, les limites de l'instrument contractuel. Le contrat ne déploie pleinement ses effets qu'à l'intérieur du périmètre que les parties peuvent juridiquement et techniquement maîtriser. Or, l'interconnexion des systèmes, la multiplication des intervenants et l'action d'acteurs extérieurs à la relation contractuelle conduisent fréquemment le risque de fraude à dépasser ce périmètre. Après avoir établi les potentialités de la gestion contractuelle, il convient donc d'en éprouver les

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

limites face à la transformation contemporaine des risques de fraude numérique.

2. Les limites de la gestion contractuelle face à la transformation des risques de fraude numérique

L'efficacité de la gestion contractuelle ne doit pas dissimuler les limites inhérentes à son champ d'action. Le contrat demeure, par nature, un instrument d'organisation de rapports juridiques déterminés, alors que le risque de fraude numérique se déploie désormais dans des environnements interconnectés associant une pluralité d'acteurs, d'infrastructures et de dépendances techniques. La structure juridique de la relation contractuelle ne coïncide donc plus nécessairement avec l'espace dans lequel le risque naît, se propage et produit ses effets.

Cette inadéquation est renforcée par les transformations économiques de l'écosystème numérique. La concentration de certaines prestations, l'opacité des architectures techniques, la multiplication des chaînes de sous-traitance et la dépendance à l'égard de prestataires difficilement substituables peuvent réduire la capacité des parties à négocier, contrôler ou faire effectivement respecter les mécanismes conventionnels de gestion du risque. Les limites du modèle apparaissent ainsi à deux niveaux. Elles sont d'abord intrinsèques, lorsque la configuration même du risque excède le périmètre que le contrat est juridiquement en mesure d'organiser. Elles deviennent ensuite fonctionnelles, lorsque l'efficacité des stipulations convenues dépend de conditions techniques, économiques ou institutionnelles que la seule volonté des parties ne suffit pas à garantir.

2.1. Les insuffisances intrinsèques du dispositif contractuel

La première série de limites résulte du décalage entre le périmètre juridique du contrat et l'environnement dans lequel se développe le risque de fraude. Alors que la convention organise des rapports déterminés entre des parties identifiables, les opérations numériques reposent fréquemment sur des chaînes d'acteurs et des infrastructures interdépendantes. Cette dissociation complique, d'une part, l'identification de l'acteur auquel la réalisation du risque peut être imputée et favorise, d'autre part, la propagation des effets d'une défaillance au-delà du périmètre conventionnel dans lequel elle a pris naissance.

2.1.1. La pluralité des acteurs et la dilution de l'imputation du risque de fraude

Une opération numérique présentée au client comme une prestation unique repose fréquemment sur une pluralité d'intervenants[17]. Ces acteurs participent techniquement à la réalisation d'un même service sans être nécessairement liés entre eux par une convention unique. Il en résulte une dissociation fondamentale entre l'unité technique de l'opération et la fragmentation juridique des relations qui la supportent. Une fraude peut affecter l'ensemble du service alors que les obligations nécessaires à sa prévention sont réparties entre plusieurs contrats. De même, une vulnérabilité située à un niveau de la chaîne peut produire des conséquences sur des acteurs avec lesquels l'entité à l'origine de la défaillance n'entretient aucun lien contractuel direct. La

[17]. À côté du prestataire directement engagé peuvent intervenir un éditeur de logiciel, un fournisseur d'infrastructure, un hébergeur, un opérateur de communications électroniques, un intégrateur, un sous-traitant chargé du traitement des données ou encore un prestataire spécialisé en sécurité

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

difficulté ne tient donc plus seulement à la détermination du contenu de l'obligation de sécurité ; elle réside dans l'identification du rapport juridique pertinent au sein d'un ensemble de relations interdépendantes.

Cette fragmentation rend particulièrement délicate l'imputation du dommage. Une même fraude peut résulter de plusieurs facteurs : une mauvaise configuration imputable au client, une vulnérabilité affectant un logiciel, l'absence d'une mise à jour attendue, la compromission d'un sous-traitant ou encore l'intervention d'un tiers malveillant. Ces causes peuvent également se combiner. L'identification d'une défaillance contractuelle suppose alors de reconstituer la chaîne technique de l'incident afin de déterminer les obligations auxquelles chaque intervenant était effectivement tenu.

Les matrices de responsabilité, les obligations de traçabilité et les mécanismes d'audit précédemment étudiés peuvent faciliter cette opération. Leur efficacité rencontre cependant une limite : l'imputation juridique dépend préalablement de la possibilité d'établir techniquement la cause de l'incident. Or, les informations nécessaires à cette démonstration sont fréquemment dispersées entre plusieurs intervenants. Les journaux d'événements peuvent être détenus par le prestataire principal, les informations relatives à l'infrastructure par un fournisseur de cloud, les données concernant une vulnérabilité par l'éditeur du logiciel et les éléments relatifs à l'attaque par d'autres opérateurs. Le cocontractant victime ne dispose pas nécessairement d'un droit d'accès direct à l'ensemble de ces informations.

La chaîne de sous-traitance accentue encore cette difficulté. Le contrat principal peut certes imposer au prestataire de

répercuter certaines exigences de sécurité sur ses propres sous-traitants. Des clauses peuvent prévoir des obligations de transparence, subordonner le recours à certains sous-traitants à une information ou à une autorisation préalable et exiger que les obligations de sécurité soient reproduites dans les contrats conclus en aval. Cette technique permet une certaine diffusion conventionnelle des exigences de sécurité à travers la chaîne.

Elle ne fait toutefois pas disparaître la fragmentation des rapports juridiques. Le bénéficiaire final du service n'est pas nécessairement partie aux contrats conclus entre son prestataire et les différents intervenants techniques. Sous réserve des mécanismes prévus par le droit applicable, le principe de l'effet relatif du contrat limite donc la possibilité d'opposer directement à un tiers les obligations issues d'une convention à laquelle il n'est pas partie. Il peut en résulter une situation paradoxale : l'acteur techniquement à l'origine de la défaillance peut se situer en dehors du rapport contractuel directement accessible à la victime. Il est vrai qu'au cœur d'un environnement économique en constante mutation, l'incertitude prévaut comme une règle omniprésente et les organisations font face à une diversité de risques[18]. Mais, la présente situation révèle l'importance croissante du risque lié aux tiers et à la chaîne d'approvisionnement numérique. Le NIST Cybersecurity Framework 2.0 intègre ainsi expressément la gestion des risques associés aux fournisseurs et aux dépendances externes dans la gouvernance de la

[18] Chaimaa ACHIR, Aziz DOUARI. Digitalisation de la gestion des risques de non recouvrementdanslesentreprises non financières: une étude qualitative desperceptions des managers de risque au Maroc. International Journal of Accounting, Finance, Auditing, Management and Economics, ,⟨10.5281/zenodo.10657625⟩. ⟨hal-04463403⟩, p. 262.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

cybersécurité[19]. Les travaux de l'ENISA consacrés aux menaces affectant les chaînes d'approvisionnement témoignent également de cette évolution[20]. Ces référentiels confirment une transformation essentielle : la sécurité d'une organisation dépend désormais, pour partie, de la sécurité d'acteurs dont elle ne maîtrise ni directement les systèmes ni entièrement les comportements.

La pluralité des acteurs révèle ainsi une première insuffisance intrinsèque de la gestion contractuelle. Le contrat peut identifier les obligations de ses parties, organiser leur coopération, encadrer le recours aux sous-traitants et répartir certaines responsabilités. Il ne peut cependant abolir la fragmentation juridique d'un écosystème dont les composantes sont techniquement interdépendantes. L'espace de production du risque devient ainsi plus large que l'espace d'imputation organisé par chaque convention.

2.1.2. La propagation des défaillances au-delà du périmètre conventionnel

La fragmentation des rapports juridiques ne rend pas seulement difficile l'imputation du risque de fraude. Elle révèle une limite plus profonde de la gestion contractuelle : le périmètre dans lequel une défaillance produit ses effets peut être beaucoup plus large que celui dans lequel le contrat déploie son autorité. L'interconnexion des systèmes, la mutualisation des infrastructures et l'utilisation de composants technologiques communs permettent à un incident localisé de se propager à une pluralité d'organisations juridiquement indépendantes. Le contrat

[19] NIST, Cybersecurity Framework 2.0, 2024, sections GV.RM-01 et GV.SC-01.
[20] *Cf.* ENISA, Rapport de l'ENISA sur le paysage des ménaces 2021.

conserve alors son utilité pour organiser la réaction de chaque partie, mais il ne peut, à lui seul, gouverner l'ensemble des effets produits en dehors de la relation qu'il encadre.

Cette propagation peut résulter de différentes formes de dépendance technique. La compromission d'un fournisseur de services cloud, l'exploitation d'une vulnérabilité affectant une bibliothèque logicielle largement utilisée, l'indisponibilité d'une infrastructure critique ou encore la compromission d'un service mutualisé peuvent affecter simultanément de nombreux utilisateurs. Une même vulnérabilité devient alors le point de départ d'incidents multiples et peut, selon les circonstances, être exploitée pour commettre des fraudes à grande échelle. La mutualisation qui procure au numérique une partie de son efficacité économique constitue ainsi également un facteur de concentration du risque.

Certes, la phase de négociation contractuelle permet de structurer l'équilibre des risques entre le client et son prestataire informatique[21]. C'est ainsi qu'une partie peut exiger de son cocontractant des mesures de sécurité, encadrer contractuellement le recours à certains sous-traitants ou imposer la répercussion de certaines obligations dans la chaîne. Mais la propagation du risque dans bien de cas, révèle ainsi les limites de la fonction préventive du contrat. Son pouvoir normatif s'amenuise à mesure que l'on s'éloigne de son périmètre conventionnel. Une partie au contrat ne peut imposer directement des mesures à tous les acteurs dont

[21] François-Xavier LANGLAIS , « Contrats informatiques : comment sécuriser les projets IT à forts enjeux ? », Le Village de la Justice, https://www.village-justice.com/articles/contrats-informatiques-comment-securiser-les-projets-forts-enjeux,56473.html

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

dépend techniquement son activité, particulièrement lorsque celle-ci repose sur des infrastructures mutualisées, des composants standardisés ou des services fournis à l'échelle mondiale.

Cette limite prend une importance particulière face au risque systémique. Celui-ci ne résulte pas seulement de la gravité intrinsèque d'un incident, mais de la possibilité qu'une défaillance affectant un élément commun se transmette à une pluralité d'acteurs interdépendants. Dans une telle configuration, l'efficacité des mesures adoptées isolément par chaque organisation ne suffit plus nécessairement à assurer la maîtrise du risque collectif. Il apparaît bien clairement que le contrat est conçu pour coordonner les intérêts et les comportements des parties qui y sont soumises ; il n'est pas, dans sa structure classique, un instrument permettant d'organiser à lui seul une réponse cohérente à l'échelle d'un écosystème numérique.

La propagation des défaillances peut également mettre à l'épreuve les catégories juridiques mobilisées pour traiter leurs conséquences. Plus les intermédiaires et les dépendances techniques se multiplient, plus il devient délicat d'articuler causalité technique, prévisibilité du dommage et causalité juridiquement pertinente. Un même événement initial peut engendrer des conséquences différentes selon l'architecture de chaque organisation, les mesures de sécurité qu'elle a adoptées ou la manière dont ses propres prestataires ont réagi. La propagation systémique ne signifie donc pas que toutes les conséquences doivent recevoir une imputation juridique identique. Elle souligne plutôt la difficulté de traiter, au moyen d'une succession de relations bilatérales, un phénomène dont les causes et les effets se déploient à une

échelle collective. Cette inadéquation explique la nécessité d'un socle normatif dépassant la seule autonomie de la volonté. Lorsque plusieurs acteurs techniquement interdépendants ne sont pas reliés par une convention commune, les obligations légales de sécurité, les mécanismes réglementaires de notification, les prescriptions sectorielles ou les standards techniques communs peuvent contribuer à rapprocher leurs comportements. Leur fonction n'est pas de se substituer systématiquement au contrat. Elle consiste notamment à imposer ou à favoriser certaines exigences communes au-delà du cercle des parties à une convention déterminée.

La norme publique et la norme contractuelle remplissent, de ce point de vue, des fonctions complémentaires. La première peut étendre la discipline à une catégorie d'acteurs indépendamment de l'existence d'un lien contractuel entre eux ; la seconde permet d'adapter cette discipline aux caractéristiques particulières d'une opération. Le contrat conserve ainsi sa fonction de précision et d'organisation des rapports individuels, tandis que les prescriptions légales et réglementaires permettent d'appréhender certains risques à une échelle que l'autonomie de la volonté ne peut atteindre seule. La propagation des défaillances ne conduit donc pas à disqualifier la gestion contractuelle. Elle permet plutôt d'en déterminer le domaine d'efficacité. Le contrat demeure particulièrement adapté à la définition des obligations, à la répartition des responsabilités et à l'organisation de la réaction entre des parties identifiées. Son aptitude diminue lorsqu'il s'agit d'imposer une discipline uniforme à des acteurs multiples ou de coordonner la réponse à une défaillance dont les effets se diffusent dans un ensemble de relations juridiquement distinctes. À mesure que le risque se

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

systémise, sa gestion ne peut plus demeurer exclusivement conventionnelle.[22]

2.2. La nécessaire articulation de la gestion contractuelle avec les exigences légales et institutionnelles de résilience numérique

Les limites de la gestion contractuelle ne résultent pas uniquement de l'incapacité du contrat à embrasser l'ensemble de l'écosystème dans lequel se développe le risque de fraude. Elles tiennent également aux conditions dans lesquelles la convention est négociée, exécutée et contrôlée. Une stipulation peut être juridiquement valable tout en demeurant faiblement négociable, difficilement vérifiable ou techniquement insuffisante. L'effectivité du dispositif contractuel dépend ainsi de facteurs que l'autonomie de la volonté ne maîtrise qu'imparfaitement.

Deux séries de difficultés apparaissent alors. D'une part, les asymétries contractuelles et les situations de dépendance technologique peuvent réduire la capacité d'une partie à négocier ou à faire effectivement respecter un niveau de protection adapté au risque (1). D'autre part, ces insuffisances montrent que la gestion contractuelle doit être replacée dans une gouvernance plus large de la sécurité et de la résilience numériques, associant prescriptions légales, régulation institutionnelle, standards techniques et coopération entre acteurs (2).

[22]TRUDEL (P.), art. préc., p. 262-270.

2.2.1. Les asymétries informationnelles et la dépendance technologique comme facteurs d'ineffectivité

L'effectivité de la gestion contractuelle du risque de fraude ne dépend pas seulement de la qualité juridique des stipulations convenues. Elle suppose également que les parties disposent d'une capacité suffisante pour négocier les obligations[23], comprendre les risques, contrôler leur exécution et, en cas de défaillance persistante, exercer effectivement les facultés que le contrat leur reconnaît. Or, les relations numériques sont fréquemment marquées par des asymétries économiques, informationnelles et techniques susceptibles de réduire chacune de ces capacités. Le contrat peut alors demeurer juridiquement valable tout en perdant une partie de son aptitude à organiser effectivement la maîtrise du risque.[24]

Cette difficulté apparaît, en premier lieu, au stade de la détermination du contenu contractuel. De nombreux services numériques, notamment ceux proposés à grande échelle, reposent sur des contrats standardisés dans lesquels les conditions de sécurité, les engagements de niveau de service, les limitations de responsabilité, les droits d'audit ou encore les modalités de réversibilité sont largement prédéterminés par le prestataire. Pour le client dont le pouvoir de négociation est limité, la liberté contractuelle ne se traduit donc pas nécessairement par la possibilité de discuter individuellement chacune des clauses. Elle peut se réduire au choix d'adhérer à l'offre proposée, de sélectionner une

[23] Un défaut de cadrage, une mauvaise expression des besoins ou une intégration défaillante peuvent entraîner des retards majeurs et des surcoûts importants. Cf. François-Xavier LANGLAIS , Op. Cit.

[24]TRUDEL (P.), art. préc., p. 259 : l'effectivité de la norme dépend du risque perçu comme émanant d'elle.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

formule différente lorsqu'elle existe ou de rechercher un autre prestataire. L'asymétrie économique peut ainsi se traduire par une asymétrie dans la maîtrise du contenu du contrat. Cette situation est particulièrement sensible lorsque les conditions générales déterminent unilatéralement les niveaux de service, les plafonds de responsabilité, les procédures de notification ou les conditions d'accès aux informations nécessaires à l'évaluation de la sécurité. L'autonomie de la volonté ne disparaît pas juridiquement ; sa portée pratique se trouve néanmoins réduite lorsque l'une des parties dispose d'une marge très faible pour adapter le dispositif contractuel à ses propres risques de fraude.

À cette première asymétrie s'ajoute, en deuxième lieu, une asymétrie informationnelle et technique. La gestion contractuelle du risque suppose que le client puisse apprécier, au moins dans une mesure suffisante, la manière dont son cocontractant exécute les obligations de sécurité souscrites. Or il ne connaît pas nécessairement l'architecture du service, la localisation des ressources, la chaîne de sous-traitance[25], les mécanismes de redondance ni les procédures de traitement des vulnérabilités et de détection des tentatives de fraude. En conséquence, il dépend largement des informations communiquées par le prestataire. Les certifications, rapports d'audit, questionnaires de sécurité, obligations de transparence et de notification, droits d'audit[26] peuvent

[25]Loi n° 2013-450 du 19 juin 2013, art. 9 et 26 : le recours à un sous-traitant et le transfert vers un pays tiers (hors CEDEAO) sont déclarés à l'Autorité de protection, qui autorise le transfert. Voir aussi loi n° 2013-546 du 30 juillet 2013, art. 7.

[26]Le droit ivoirien n'impose aucun droit d'audit, qui relève de la liberté contractuelle. Le responsable du traitement doit toutefois choisir un sous-traitant

réduire cette asymétrie. Mais ils ne garantissent pas un accès exhaustif à l'information car des contraintes de sécurité, de confidentialité, de protection des autres clients ou d'organisation technique peuvent en limiter le périmètre[27]. Le contrat organise ainsi la transparence sans supprimer l'avantage informationnel structurel du prestataire. Cette asymétrie affecte directement l'effectivité du dispositif car une obligation se contrôle difficilement sans les informations nécessaires à son appréciation. De même une fraude peut révéler a posteriori des dépendances ou des vulnérabilités que le client n'avait pu identifier à la formation du contrat[28]. L'efficacité de la stipulation dépend alors autant de sa précision juridique que de l'accessibilité des éléments techniques permettant d'en vérifier l'exécution.

En troisième lieu, l'effectivité du contrat peut être affectée par une dépendance technologique susceptible de réduire la capacité réelle de substitution du prestataire. Les formats propriétaires, les coûts de migration, la complexité des architectures, l'intégration profonde d'un service dans les processus de l'entreprise, les besoins de reconfiguration des applications ou encore la disponibilité des compétences nécessaires au changement peuvent rendre la sortie juridiquement possible mais économiquement ou techniquement difficile. Le phénomène de verrouillage

offrant des garanties suffisantes et veiller à leur respect (loi n° 2013-450, art. 20 et 40). Audit et certification par l'ARTCI : loi n° 2013-546, art. 50.

[27]Loi n° 2024-352 du 6 juin 2024, art. 75, al. 2 et art. 77, al. 3 : la communication d'informations peut être limitée pour des motifs de sécurité des réseaux ou de secret des affaires ; ce dernier n'est toutefois pas opposable à l'ARTCI (art. 159). Voir aussi loi n° 2013-450, art. 19 (confidentialité des données personnelles).

[28]Loi n° 2024-352, art. 98 et 99 : l'opérateur informe l'ARTCI et les abonnés concernés en cas d'incident de sécurité significatif, et l'ARTCI peut commanditer un audit. Sur la traçabilité des accès aux données : loi n° 2013-450, art. 41, 8e tiret.

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

technologique, ou vendor lock-in, révèle ainsi une distinction importante entre liberté juridique de résiliation et capacité effective de substitution. Une partie peut disposer contractuellement du droit de mettre fin à la relation sans être matériellement en mesure de l'exercer dans des conditions raisonnables. Plus l'activité de l'entreprise dépend d'un service particulier, plus le coût du changement peut réduire la crédibilité de la faculté de sortie. Cette dépendance peut avoir une incidence directe sur la gestion du risque de fraude. Lorsqu'un incident révèle des insuffisances persistantes dans les dispositifs de sécurité d'un prestataire, le client peut théoriquement disposer de moyens contractuels lui permettant d'exiger une remédiation, voire de mettre fin à la relation. Mais si le coût technique et économique du changement est particulièrement élevé, l'exercice de ces prérogatives peut être différé ou devenir difficile. Le verrouillage technologique ne supprime donc pas nécessairement les droits contractuels ; il peut affaiblir leur effectivité pratique.

Ces asymétries sont particulièrement marquées lorsque l'entreprise cliente dispose de ressources techniques, juridiques ou organisationnelles limitées. Concevoir et suivre un dispositif contractuel de gestion du risque[29] exige en effet de savoir apprécier les exigences de cybersécurité, comprendre les architectures numériques, évaluer les

[29]Les droits et obligations de l'entité financière et du prestataire TIC sont clairement répartis et énoncés par écrit, dans un document unique incluant les niveaux de service. *Cf.* Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, JOUE L 333, 27.12.2022, art. 30, § 1

audits[30], négocier la responsabilité et réagir à un incident. Lorsque ces compétences font défaut, la sophistication du contrat peut excéder la capacité réelle de l'organisation à en mobiliser les mécanismes. Le droit peut certes corriger certaines situations : selon la relation et les textes applicables, le droit de la consommation, le droit de la concurrence ou d'autres protections peuvent encadrer certaines pratiques ou stipulations[31]. Mais ces correctifs restent insuffisants. Les régimes varient selon la qualité des parties et la nature de l'opération, et rééquilibrer juridiquement le contrat ne supprime pas nécessairement l'asymétrie technique ni la dépendance technologique qui pèsent concrètement sur la relation. Il faut donc dépasser une conception purement conventionnelle de la gestion du risque. Le contrat reste indispensable pour préciser les obligations des parties et adapter les exigences de sécurité à chaque opération[32], mais son efficacité suppose aussi des règles communes, des mécanismes de contrôle, des institutions compétentes et des capacités organisationnelles[33]. La question n'est plus

[30]Pour les services soutenant des fonctions critiques ou importantes, le contrat prévoit des droits d'accès, d'inspection et d'audit au profit de l'entité financière, d'un tiers désigné par elle et de l'autorité compétente.. *Cf.* Règlement (UE) 2022/2554, *préc.*, art. 30, § 3, e)

[31]*Cf.* Loi n° 2024-352 du 6 juin 2024, art. 7 sur pratiques anticoncurrentielles prohibées et art. 106 à 109 sur l'information du consommateur, modification des conditions contractuelles et résiliation sans frais ; loi n° 2013-546 du 30 juillet 2013, art. 8, al. 2, 1 : le choix de la loi applicable ne peut priver le consommateur de la protection du droit ivoirien.

[32] Règlement (UE) 2022/2554, *préc.*, art. 30, § 2, a) : le contrat décrit de façon claire et complète les fonctions et services TIC fournis, et indique si la sous-traitance est permise et à quelles conditions.

[33]Loi n° 2024-352, art. 97 et 141 : l'ARTCI définit le niveau de sécurité minimal exigé des opérateurs et contrôle le respect de leurs obligations, sous peine de sanctions (Titre X). Elle est aussi l'Autorité de protection des données (loi n°

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

seulement d'améliorer le contenu du contrat, mais de l'inscrire dans un dispositif plus large, capable de compenser ses insuffisances et d'assurer la continuité de la gestion du risque au-delà de la relation conventionnelle. Cela conduit à envisager son inscription dans une gouvernance intégrée de la résilience numérique.

2.2.2. L'inscription du contrat dans une gouvernance intégrée de la résilience numérique

Les limites précédemment mises en évidence n'écartent pas la gestion contractuelle du risque de fraude ; elles conduisent à la situer dans un dispositif plus large. Dès lors que le risque déborde le périmètre conventionnel et que l'effectivité des stipulations dépend de conditions que les parties ne maîtrisent pas entièrement, le contrat n'est pas un instrument autosuffisant. La norme légale fixe des exigences obligatoires ; les autorités compétentes en assurent, dans la limite de leurs attributions, la mise en œuvre ou le contrôle. Les référentiels techniques objectivent les pratiques attendues et le contrat en adapte la portée aux caractéristiques de l'opération. Il agit ainsi comme un relais de la régulation dans les relations économiques, et non comme une alternative à celle-ci. Cette articulation s'inscrit dans le passage d'une logique de sécurité à une logique de résilience numérique. La première vise surtout à prévenir l'atteinte et à réduire la probabilité du risque. La seconde y ajoute la capacité d'une organisation à absorber l'incident, à maintenir ou rétablir ses fonctions essentielles et à adapter son dispositif à l'expérience

2013-450 du 19 juin 2013, art. 46) et audite les systèmes d'information (loi n° 2013-546, art. 50).

acquise[34]. Le risque de fraude n'est plus seulement un événement à empêcher ; c'est aussi une éventualité dont les conséquences doivent pouvoir être contenues.

Le contrat y contribue par les engagements de niveau de service, les mécanismes de continuité et de reprise, les obligations de sauvegarde, les procédures de notification et de coopération et les clauses de réversibilité. Ensemble, ils organisent un continuum de la prévention à la restauration. Cette contribution demeure toutefois limitée par l'effet relatif du contrat : il n'oblige que ses parties et ne peut organiser la conduite d'acteurs qui n'y sont pas liés[35]. En effet, la continuité d'une entreprise peut encore être compromise par la défaillance d'un fournisseur critique, l'indisponibilité d'une infrastructure de communication, la compromission d'un composant largement diffusé ou l'interruption d'un service numérique essentiel. Donc, à l'interdépendance des risques doit répondre une coordination des moyens de les maîtriser : détection et assistance, partage d'informations, procédures communes en cas d'incident, référentiels partagés et supervision sectorielle[36]. Car, si le contrat précise les obligations d'une relation donnée, il ne se substitue pas aux mécanismes qui coordonnent des acteurs non liés par une

[34]NIST, Special Publication 800-160, Volume 2, Revision 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*, décembre 2021, p. 58 : la « cyber resiliency » y est définie comme « the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources ». DOI : 10.6028/NIST.SP.800-160v2r1.

[35] Art.1134 du code civl ivoirien : les conventions légalement formées tiennent lieu de loi à ceux qui les ont faites.

[36]Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (directive SRI 2), considérants 85 et 90 et article 21, paragraphe 2, points c) et d), JOUE L 333, 27 décembre 2022, p. 80.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

même convention. En tout état de cause, la gouvernance intégrée du risque repose sur la complémentarité des instruments, et non sur leur concurrence.

En droit ivoirien, cette articulation s'appuie sur plusieurs ensembles normatifs : la protection des données à caractère personnel, qui impose des exigences de sécurité des traitements, la répression de la cybercriminalité et le droit des communications électroniques, qui encadre la sécurité et la continuité des réseaux et services[37]. La stipulation contractuelle peut y préciser les comportements attendus des parties sans se substituer aux obligations légales. La dimension institutionnelle complète ce cadre : les autorités de régulation et les structures nationales de cybersécurité assurent, selon leurs attributions, prévention, contrôle, assistance et coordination, et offrent des références communes que le contrat transforme en obligations adaptées à l'opération[38]. Cette gouvernance doit toutefois rester évolutive, car les techniques frauduleuses, les vulnérabilités et les dépendances technologiques changent. Le contrat y contribue par des clauses de révision, des audits périodiques ou l'actualisation des annexes techniques, nourries par les informations extérieures à la relation : référentiels, alertes de

[37]Loi n° 2013-450 du 19 juin 2013, art. 40 et 41 (mesures de sécurité du traitement) ; loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ; loi n° 2024-352 du 6 juin 2024, art. 97 et 98 (sécurité et continuité des réseaux et services).

[38]Loi n° 2024-352, art. 141 : l'ARTCI contrôle le respect des obligations des opérateurs et peut sanctionner (Titre X) ; elle audite les systèmes d'information (loi n° 2013-546 du 30 juillet 2013, art. 50) et coopère avec ses homologues de la CEDEAO et de l'UEMOA (loi n° 2024-352, art. 163).

sécurité, prescriptions des autorités[39]. Plus le risque devient systémique, plus l'efficacité du contrat dépend de son insertion dans un système de normes et d'institutions qui dépasse les parties. Ne pouvant gouverner seul le risque, il en organise la maîtrise à l'échelle de la relation tout en s'articulant avec les dispositifs collectifs de résilience. L'effectivité de la gestion juridique de la fraude numérique se joue dans cette articulation entre autonomie contractuelle et gouvernance collective.

Conclusion

Au terme de cette étude, la gestion contractuelle du risque de fraude numérique, entendue comme l'atteinte commise par des moyens numériques et non comme la fraude affectant la formation des contrats conclus par voie électronique, fait apparaître un déplacement de la fonction du contrat. Instrument classique de prévision et d'allocation des risques, il devient, dans l'environnement numérique, un moyen d'en organiser la maîtrise. Il permet d'en identifier et d'en anticiper la réalisation, de préciser les obligations de sécurité et de détection, d'en répartir les conséquences et de préparer la réponse à l'incident ainsi que la continuité de l'activité. En droit ivoirien, cette fonction s'adosse aux exigences issues notamment des législations relatives à la protection des données à caractère personnel, à la cybercriminalité et aux communications électroniques. Le contrat en traduit les

[39]Loi n° 2024-352, art. 97, al. 2 : les mesures de sécurité doivent être adaptées au risque existant au regard des normes en vigueur ; art. 98 : l'opérateur rend compte à l'ARTCI des causes de l'incident et des mesures prises pour éviter sa résurgence.

Received: 02/08/2026 Accepted: 03/09/2026 Published: 22/10/2026

prescriptions générales en obligations ajustées aux caractéristiques de chaque opération.

Nonosbtant cette capacité d'organisation, le contrat ne saurait prétendre à une maîtrise complète du risque. Sa limite ne signifie pas non plus son inutilité, mais plutôt son insuffisance lorsqu'il prétend gouverner seul un risque systémique. L'interconnexion des systèmes, les chaînes de sous-traitance, les dépendances logicielles et les infrastructures partagées font naître et circuler la fraude dans un espace qui excède fréquemment celui où le contrat produit ses effets. Les asymétries informationnelles et économiques, l'opacité technique et la dépendance technologique en affaiblissent encore l'effectivité. Le contrat doit dès lors être saisi non comme un modèle autosuffisant, mais comme l'un des instruments d'une gouvernance intégrée. Sa force propre est d'adapter les exigences de sécurité à une opération déterminée, de fixer les responsabilités, d'en organiser le contrôle et de préparer les comportements attendus lorsque le risque se réalise. Les normes impératives, la régulation institutionnelle, les référentiels techniques et les mécanismes de coopération appréhendent, pour leur part, ce qui échappe à la seule autonomie de la volonté.

Cette articulation inscrit ainsi la gestion contractuelle dans une logique de résilience numérique. L'impossibilité d'éliminer entièrement la fraude impose non seulement de la prévenir, mais encore d'en absorber les effets, de maintenir les fonctions essentielles, de rétablir l'activité et d'adapter les dispositifs à l'évolution des menaces. Le contrat y participe lorsqu'il cesse de figer des obligations au jour de sa conclusion pour en organiser la réévaluation, le contrôle et l'adaptation dans le temps. Technique nécessaire et

structurellement incomplète, la gestion contractuelle tire précisément son intérêt doctrinal de cette tension. Elle conduit à dépasser l'alternative entre confiance dans l'autonomie contractuelle et intervention de la régulation. En tout état de cause, la gouvernance intégrée du risque repose sur la complémentarité des instruments, et non sur leur concurrence. Le contrat n'en est ni la frontière ni le terme, mais un point d'articulation entre la prévention individuelle et la résilience collective.

Bibliographie

Ouvrages et articles doctrinaux

BARTHÉLEMY (B.) et COURRÈGES (Ph.), Gestion des risques. Méthode d'optimisation globale, 2e éd., Éditions d'Organisation / Eyrolles, 2004, 482 p.

BELLAYER-LE COQUIL (R.), « Le droit et le risque. Illustration avec le droit de la responsabilité civile », ATALA, n° 5, 2002, 28 p.

BERGEL (J.-L.), « La sécurité juridique », Revue du notariat, vol. 110, n° 2, septembre 2008, p. 271-285 (16 p.). En ligne : https://doi.org/10.7202/1045538ar

BILE-AKA (J.), « Libres propos sur la gestion du risque juridique en entreprise », IIIe édition du Congrès africain des juristes d'entreprises (COJA 2010), 2010, 11 p.

CALABRESI (G.), The Costs of Accidents. A Légal and Economie Analysis. In: Revue internationale de droit comparé. Vol. 22 N°2, Avril-juin 1970. pp. 410-411;

ÇELEBİ (Ö.), « Théorie des risques en droit français », Ankara Üniversitesi Hukuk Fakültesi Dergisi, vol. 69, n° 1, 2020, p. 57-106 (50 p.).

Received: 02/08/2026 **Accepted:** 03/09/2026 **Published:** 22/10/2026

CORNU (G.) (dir.), Vocabulaire juridique, 12e éd., PUF, 2018, 1100 p.

ESPESSON-VERGEAT (B.), Le droit des contrats à l'épreuve du numérique, LGDJ, 2022.

FRISON-ROCHE (M.-A.), La compliance, Dalloz, 2022.

GHESTIN (J.), Traité de droit civil. La formation du contrat, 4e éd., LGDJ, 2013.

GUINCHARD (S.) et DEBARD (T.), Lexique des termes juridiques, Dalloz, 21^(e) édition, 2014, 983 p.

https://www.persee.fr/doc/ridc_0035-3337_1970_num_22_2_15727

MOATTI (A.), « Le numérique rattrapé par le digital ? », Le Débat, 2016/1, n° 188, p. 68-72 (6 p.).

MOISAN (P.), « Technique contractuelle et gestion des risques dans les contrats internationaux : les cas de force majeure et d'imprévision », Les Cahiers de droit, vol. 35, n° 2, 1994, p. 281-334.

PICHONNAZ (P.), Impossibilité et exorbitance : étude analytique des obstacles à l'exécution des obligations en droit suisse (art. 119 CO et 79 CVIM), Editions universitaires, Travaux de la faculté de droit de l'Université de Fribourg, Fribourg 1997, n° 44

TERRÉ (F.), SIMLER (Ph.), LEQUETTE (Y.), Droit civil. Les obligations, 12e éd., Dalloz, 2018.

TRUDEL (P.), « Le risque, fondement et facteur d'effectivité du droit », p. 243-271.

VIVANT (M.), BRUGUIÈRE (J.-M.), Droit du numérique, 3e éd., Dalloz, 2022.

VOIDEY (N.), Le risque en droit civil, PUAM, Aix-en-Provence, 2005.

Rapports et documents techniques

ANSSI (France), Retour d'expérience sur l'incendie du datacenter OVHcloud, rapport technique, 2021.

CISA, Analysis of the SolarWinds Incident, 2021.

ENISA, Rapport de l'ENISA sur le paysage des ménaces 2021.

OCDE, Digital Security Risk Management, 2023.

Banque mondiale, Digital Development Overview, 2021.

Textes juridiques

Côte d'Ivoire, loi n° 2024-325 du 6 juin 2024 relative aux communications électroniques.

Côte d'Ivoire, loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Côte d'Ivoire, loi n° 2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité.

Côte d'Ivoire, loi n° 2013-546 du 30 juillet 2013 relative aux transactions électroniques.

Côte d'Ivoire, décret n° 2021-916 du 22 décembre 2021 portant Référentiel général de sécurité des systèmes d'information (RGSSI).

Côte d'Ivoire, décret n° 2024-958 du 30 octobre 2024 portant création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Union africaine, Convention sur la cybersécurité et la protection des données à caractère personnel (Convention de Malabo), 27 juin 2014.

Union Européenne, Règlement 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier, JOUE L 333, 27.12.2022, pp. 1-79