

De l'injection de faute en droit

Premiers jalons pour une analyse juridique

François Viangalli

Maître de conférences HDR à l'Université Grenoble-Alpes

CYBERALPS - Lab. CESICE



Cybersecurity Institute
Univ. Grenoble Alpes



Que signifie l'expression *Injection de faute* ?

Iniectio est issue du verbe *inicere*, qui signifie « *jeter dans* » ou « *mettre sur* »

Faute, du latin populaire *fallita*, issu du verbe *fallere*, qui signifie « *tromper* » ou « *faire défaut* » ; à rapprocher de *falsus*, « *faux* », participe passé du même verbe.

Littéralement, cela signifie : *jeter une tromperie*

L'injection de fautes (IF) – *vitii iniectio*, si l'on devait l'exprimer en latin classique – existait déjà, dans son principe ou par analogie, dans l'Antiquité biblique et dans le monde gréco-romain.

Trois exemples en témoignent :

- La *Vigne de Naboth*
- Le *Faux Prophète Alexandre*
- La *Lex Cornelia de falsis*

La Vigne de Naboth, Premier Livre des Rois (1 R 21, 8-13)

Le roi Achab convoite la vigne de Naboth, qui refuse de la lui céder.

La reine Jézabel écrit des lettres au nom d'Achab et les scelle du sceau royal.

Elles ordonnent aux anciens de la ville de produire de faux témoins, qui accusent Naboth d'avoir maudit Dieu et le roi.

Sur cette base, Naboth est condamné et lapidé. Achab, dès lors, prend possession de la vigne.

L'injection procède ainsi :

- Utilisation frauduleuse du sceau par une personne qui y a accès ;
- Exploitation de l'autorité attachée à l'ordre scellé, que nul ne songe à contester.

Lucien de Samosate, *Alexandre ou le faux prophète* (vers 180 apr. J.-C.)

Un charlatan, Alexandre d'Abonotique, se fait passer pour un oracle. Les fidèles lui soumettent leurs questions sur des tablettes scellées. Alexandre leur répond sans paraître briser le sceau, ce qui le fait passer à leurs yeux pour un envoyé des dieux.

Un expert, Lucien, dévoile les procédés employés par le charlatan (§ 21) :

- Décollement de la cire avec une aiguille chauffée, puis recollage ;
- Prise d'empreinte du sceau et fabrication d'un faux sceau identique.

Il éprouve ensuite l'oracle avec des tablettes scellées de manière à rendre toute ouverture détectable, et démasque publiquement Alexandre (§ 53-54).

Furieux, Alexandre tente de le faire jeter à la mer par l'équipage du navire qu'il lui a fourni (§ 55-56). Lucien veut alors le poursuivre en justice, mais le gouverneur l'en dissuade (§ 57).

Le schéma est le suivant :

- Injection de faute matérielle (attaque physique du sceau) ;
- Exploitation des données ;
- Analyse de la vulnérabilité ;
- Renforcement du système ;
- Publication du résultat ;
- Représailles contre le chercheur.

« ἕτερος δὲ τρόπος ὁ διὰ τοῦ λεγομένου **κολλυρίου**· σκευαστὸν δὲ τοῦτό ἐστιν ἐκ πίττης Βρεττίας καὶ ἀσφάλτου καὶ λίθου τοῦ διαφανοῦς τετριμμένου καὶ κηροῦ καὶ μαστίχης. [...] ἐκ γὰρ τούτων ἀπάντων ἀναπλάσας τὸ κολλύριον καὶ θερμήνας πυρί, σιάλῳ τὴν σφραγίδα προχρίσας ἐπετίθει καὶ ἀπέματτε τὸν τύπον.»

« *Une autre méthode employait ce qu'on appelle le **kollyrion**, une préparation de poix du Bruttium, d'asphalte, de pierre transparente broyée, de cire et de mastic. Il en façonnait une pâte, la chauffait au feu, l'appliquait sur le sceau préalablement humecté de salive, et en prenait l'empreinte. La pâte durcissait aussitôt : **il ouvrait alors les rouleaux, les lisait, remettait la cire et y imprimait un sceau exactement semblable à l'original**, comme on le ferait avec une pierre gravée.* »

Lucien, *Alexandre ou le faux prophète*, § 21. Texte grec : éd. A. M. Harmon, Loeb Classical Library, 1925.

Le droit romain : la Lex Cornelia de falsis (81 av. J.-C.)

La loi Cornelia, votée sous Sylla, réprime déjà comme un crime la falsification des actes, y compris par l'usage d'un faux sceau. Selon les *Institutes* de Justinien (IV, 18, 7), la peine est la déportation pour les hommes libres et le dernier supplice pour les esclaves.

*Lege Cornelia testamentaria obligatur, qui **signum adulterinum** fecerit aut sculpserit.*

« Tombe sous le coup de la loi Cornelia testamentaire celui qui aura fabriqué ou gravé **un sceau contrefait**. »

Modestin, *Digeste*, 48, 10, 30

L'INJECTEUR

L'INJECTÉ

L'ALTÉRATION

LA PREUVE

LA RESPONSABILITÉ

L'INJECTEUR

Droit français

Lorsqu'elle vise le système d'autrui sans autorisation, l'IF peut être constitutive d'un délit d'atteinte à un système de traitement automatisé de données (STAD), au sens des articles 323-1 et suivants du Code pénal.

Ces textes répriment, de peines d'emprisonnement pouvant aller jusqu'à dix ans (art. 323-4-1) :

- L'accès ou le maintien frauduleux dans un STAD (art. 323-1) ;
- L'entrave au fonctionnement d'un STAD (art. 323-2) ;
- L'introduction, l'extraction, la modification ou la suppression frauduleuse de données (art. 323-3) ;
- La détention ou la mise à disposition de moyens conçus pour commettre ces infractions (art. 323-3-1).

L'accès du responsable à son propre système, n'est pas frauduleux.

Les atteintes des articles 323-1 à 323-3 ne peuvent être reprochées à celui qui dispose des droits sur le système, y compris des droits de propriété intellectuelle. Le chercheur qui injecte une faute dans une puce qui lui appartient ne commet donc pas d'accès frauduleux, du moins **lorsqu'il dispose des droits d'accès et de modification** nécessaires sur le système testé.

Par voie de conséquence, l'infraction de l'article 323-3-1 ne peut être caractérisée à raison de moyens destinés à être employés par celui qui a des droits sur le système.

L'IF peut parfois être licite, lorsqu'elle est réalisée pour motif légitime

Article 323-3-1 du Code pénal

*« **Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique,** d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »*

Ce fait justificatif n'est toutefois admis par la loi qu'en matière de délits d'importation, détention, offre, cession ou mise à disposition des outils ou données.

Que faut-il entendre par *recherche* ou *sécurité informatique* ?

La jurisprudence est mince, et le seul arrêt de référence est antérieur à l'ajout de ces mots dans le texte de la loi.

Chambre criminelle, 27 octobre 2009, n° 09-82.346

« Attendu qu'il résulte de l'arrêt attaqué et des pièces de procédure que **X a diffusé sur le portail internet de la société XX Consulting, spécialisé dans le conseil en sécurité informatique, dont il est le gérant, des écrits directement visibles sur le site et accessibles à tous permettant d'exploiter des failles de sécurité informatique** ; que, renvoyé devant le tribunal correctionnel pour mise à disposition, sans motif légitime, de moyens conçus ou spécialement adaptés pour commettre une atteinte à un système de traitement automatisé de données, il a été relaxé ; Attendu que, pour infirmer, sur appel du ministère public, le jugement et condamner le prévenu, l'arrêt énonce qu'il ne peut valablement arguer d'un motif légitime tiré de la volonté d'information, dès lors que, **du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance** ; Attendu qu'en l'état de ces énonciations, abstraction faite du motif surabondant relatif aux antécédents judiciaires du prévenu, et dès lors que **la constatation de la violation, sans motif légitime et en connaissance de cause, de l'une des interdictions prévues par l'article 323-3-1 du code pénal implique de la part de son auteur l'intention coupable exigée par l'article 121-3 du même code, la cour d'appel a justifié sa décision (...).** »

Chambre criminelle, 7 janvier 2020, n° 18-84.755

« L'administration fiscale a indiqué avoir découvert, **au sein d'officines de pharmacies**, que ce **logiciel** intégrait une fonctionnalité **permettant**, après saisie d'un mot de passe personnel, **de faire disparaître des lignes d'écritures relatives à des ventes payées en espèces**, à la condition qu'elles ne soient pas liées à une prescription médicale ou au paiement d'un tiers, avant qu'elles ne soient arrêtées d'un point de vue comptable. Par ailleurs, **une manipulation externe** au logiciel, effectuée directement en ligne de commande, **permettait de détruire les traces de ces effacements** par simple suppression du fichier qui les contient. (...) Pour confirmer l'ordonnance ayant dit n'y avoir lieu à suivre, l'arrêt retient que le logiciel conçu et commercialisé permettait à son acquéreur, propriétaire des données, de faire disparaître des lignes d'écriture relatives à des ventes payées en espèces, avant qu'elles ne soient arrêtées d'un point de vue comptable. Les juges en déduisent que l'infraction prévue à l'article 323-3-1 du code pénal ne peut être reprochée aux sociétés Alliance software et Alliadis, dès lors que celles prévues aux articles 323-1 à 323-3 ne peuvent être caractérisées. En l'état de ces énonciations, la chambre de l'instruction a justifié sa décision. »

(...)

En effet, les atteintes aux systèmes de traitement automatisé de données prévues aux articles 323-1 à 323-3 du code pénal ne sauraient être reprochées à la personne qui, bénéficiant des droits d'accès et de modification des données, procède à des suppressions de données, sans les dissimuler à d'éventuels autres utilisateurs du système. »

En l'état, on peut raisonnablement soutenir que le motif légitime couvre :

- La recherche publique ou privée, menée sans atteinte à des systèmes tiers ;
- La publication scientifique évaluée par les pairs, par opposition à la diffusion d'outils prêts à l'emploi sur un site ouvert à tous.

L'IF peut aussi échapper au champ d'application de l'article 40 du Code de procédure pénale, si elle se traduit *in fine* par un **signalement de vulnérabilité à l'ANSSI** par une personne de bonne foi (article L. 2321-4 du Code de la défense).

Enfin, **la rétro-ingénierie est licite**, si bien que l'étude des vulnérabilités d'un système acquis à cette fin n'est pas par principe prohibée, **sauf clause contraire ou disposition légale particulière** (art. L. 151-3 du Code de commerce).

Droit européen

La liberté de la recherche scientifique est protégée par la Charte des droits fondamentaux.

Art 13 CDFUE :

« Les arts et la recherche scientifique sont libres. La liberté académique est respectée. »

Elle l'est aussi par l'article 10 de la Convention européenne des droits de l'homme, relatif à la liberté d'expression, pour la publication des travaux de recherche, **sous réserve du devoir de mesure** qui pèse sur le chercheur, spécialement dans les matières sensibles.

Le devoir de mesure s'apprécie **selon la qualité de la personne** : CEDH *Hadjianastassiou c. Grèce* (1992) n° 12945/87.

NB : Dans cette affaire, un ingénieur, capitaine dans l'armée de l'air grecque et responsable d'un programme de missile guidé, avait transmis contre rémunération à une société privée une étude technique sur les missiles guidés. Il avait été condamné à cinq mois d'emprisonnement en appel pour divulgation d'informations militaires. La Cour ne constata pas de violation de l'article 10 : la divulgation de connaissances techniques sur une arme pouvait en effet nuire à la sécurité nationale, et le requérant était tenu, comme militaire, à une obligation de discrétion (§ 45-47).

Ceci ne concerne que les *tests mandatés* et non *a priori* les attaques isolées à la propre initiative personnelle du chercheur, dont le cas n'est pas tranché (Considérant 17 de la Directive 2013/40 relative aux attaques des SI).

En d'autres termes, c'est la fonction qui est protégée par le mandat, et non le chercheur en tant que personne.

Il y a là un **fait justificatif**, et **non une immunité personnelle**.

Droit international

La liberté de la recherche est protégée par le *Pacte international relatif aux droits économiques, sociaux et culturels*.

Article 15 § 3

« *Les États parties au présent Pacte s'engagent à respecter la liberté indispensable à la recherche scientifique et aux activités créatrices.* »

La Convention de Budapest sur la cybercriminalité du Conseil de l'Europe (2001), ratifiée par la France, exclut de l'incrimination des « *dispositifs* » ceux qui sont produits ou détenus pour des essais autorisés ou la protection d'un système (art. 6, § 2).

L'INJECTÉ

L'injecté est soumis, comme tout responsable d'un système d'information, à une obligation de cybersécurité (ODC).

Trois textes essentiels font peser sur lui cette obligation :

- Le RGPD qui requiert des mesures techniques et organisationnelles *appropriées* (art. 24, 25 et 32) ;
- La Directive NIS2 (2022), qui requiert des mesures *appropriées et proportionnées*, compte tenu de l'état de l'art (art. 21) ;
- Le Règlement sur la cyber-résilience (2024), article 13 et annexe I : qui requiert une conception et mise sur le marché de produits offrant un niveau de cybersécurité *approprié*.

NB : Le règlement sera entièrement applicable le 11 décembre 2027.

L'obligation de cybersécurité est en principe une obligation de moyens, car aucune protection ne couvre toutes les attaques, *a fortiori* celles qui atteignent le matériel lui-même.

Lorsque des données personnelles sont en cause, c'est une **obligation de moyens renforcée** : c'est au responsable du traitement de prouver qu'il a pris des mesures appropriées (article 82 RGPD).

Pour la Cour de justice, une attaque réussie ne suffit pas, à elle seule, à établir que les mesures étaient inappropriées ; mais c'est au responsable du traitement de prouver qu'elles l'étaient.

L'obligation de cybersécurité n'est donc pas en tant que telle une obligation d'inviolabilité.

CJUE *Natsionalna agentsia za prihodite* (2023) C-340/21

NB : La distinction classique entre l'obligation de moyens et l'obligation de résultat est connue en droit français ; pas, du moins explicitement, en droit européen, même si le raisonnement y est analogue.

L'obligation de cybersécurité est **appréciée** dans son contenu *in concreto* par le juge, lequel peut prendre en considération des référentiels.

La plupart des référentiels sont dépourvus de valeur impérative.

Parmi ceux-ci, on peut citer :

- Le *Référentiel général de sécurité* (décret n° 2010-112), obligatoire pour les administrations ;
- Le *Référentiel Cyber France* (ReCyF), pour la mise en œuvre de NIS2, qui énonce 20 objectifs de sécurité et des *moyens acceptables de conformité*, non obligatoires.

La résistance physique des composants, quant à elle, est évaluée dans le cadre de la certification des produits en fonction du *potentiel d'attaque*.

(CSPN, Critères Communs, schéma européen EUCC – règlement d'exécution (UE) 2024/482)

Pour attester de la robustesse des produits, le règlement sur la cyber-résilience (2024) impose, entièrement applicable à partir du 11 décembre 2027, une évaluation de conformité et un marquage CE.

Le règlement prévoit de telles évaluations et marquages, selon le système suivant :

- Pour les **produits courants**, le fabricant s'autoévalue (**contrôle interne**) ;
- Les **produits importants et critiques** sont soumis à des **exigences renforcées** (définies par les annexes III et IV) ;
- Les **microprocesseurs et microcontrôleurs résistants** aux manipulations (produits importants de classe II) doivent être **évalués par un tiers, organisme notifié, ou détenir un certificat européen** ;
- Les **produits critiques** – cartes à puce, éléments sécurisés, modules matériels de sécurité – pourront être soumis à l'**obtention obligatoire d'un certificat européen de cybersécurité** de niveau au moins « *substantiel* ».

L'ALTÉRATION

L'IF peut provoquer :

- Un arrêt du système ;
- Une destruction du système ;
- Une fuite de données ;
- Une falsification.

Le cas de la falsification est particulièrement remarquable.

En effet, lorsque l'IF compromet le dispositif de création de signature, elle permet de produire un acte électronique signé avec le bon dispositif, mais qui n'émane pas de son titulaire. C'est la forme moderne de la *Vigne de Naboth*.

La présomption de fiabilité de la signature électronique qualifiée peut alors être exploitée à des fins frauduleuses :

- **Par l'auteur de l'acte**, qui s'attaque lui-même pour se ménager un moyen de désaveu pour l'avenir (**théorie de l'acte miné**); l'adage *nemo auditur propriam turpitudinem allegans* lui est en principe opposable, encore faut-il prouver l'auto-attaque ;
- **Par le tiers injecteur**, qui se prévaut de l'acte falsifié (**théorie de la Vigne de Naboth**).

Le règlement eIDAS ne pose pas, pour la signature électronique, de présomption de validité, mais **un principe d'équivalence**.

En vertu de ce principe, **la signature électronique qualifiée a un effet juridique équivalent à celui d'une signature manuscrite** (art. 25, § 2).

Les présomptions qu'il édicte expressément visent d'autres services : cachet électronique qualifié (art. 35, § 2), horodatage qualifié (art. 41, § 2).

Il renvoie pour le reste au droit national (considérant 49).

En droit français, le Code civil dispose que **la fiabilité du procédé est présumée jusqu'à preuve contraire** (art. 1367, al. 2). Le décret n° 2017-1416 attache cette présomption à la signature électronique qualifiée.

La présomption est réfragable.

L'utilisation d'un instrument de paiement telle qu'enregistrée par le prestataire ne suffit pas nécessairement à prouver que l'opération a été autorisée par le payeur (art. L. 133-23 du Code monétaire et financier).

NB : La signature et le paiement reposent souvent sur des puces de même nature, d'un point de vue technique. Juridiquement, les deux opérations sont distinctes.

LA PREUVE

De lege lata, la principale difficulté dans l'administration de la preuve d'une IF résulte du caractère souvent indétectable de l'injection elle-même.

C'est pourquoi deux types de preuve méritent d'être distingués :

- **La preuve intrinsèque**, par démonstration technique de l'IF et de son résultat ;
- **La preuve extrinsèque**, par démonstration circonstanciée du caractère faux ou invraisemblable de l'acte issu d'une IF.

La preuve intrinsèque porte sur l'*instrumentum*, la preuve extrinsèque sur le *negotium*.

Elle est la plus convaincante, mais aussi la plus difficile à établir, car elle peut se heurter à deux obstacles :

- **Un obstacle technique** : en l'état de l'art, une IF peut ne laisser aucune trace ;
- **Un obstacle juridique** : démontrer l'IF peut exiger l'accès à la conception du composant, à ses contre-mesures et à ses rapports d'évaluation, protégés par le secret des affaires et parfois situés à l'étranger.

En droit français, le juge peut faire usage de ses pouvoirs reconnus par loi pour surmonter ces obstacles :

- Il peut ordonner des mesures d'instruction *in futurum* (art. 145 du Code de procédure civile) et ordonner la production forcée de pièces (art. 11) ;
- Procéder à l'examen des pièces par lui seul, hors la présence du public, pour protéger le secret des affaires (art. L. 153-1 du Code de commerce).

Au sein de l'Union européenne, si des éléments de preuve se trouvent dans un autre État membre, le règlement *Obtention de preuve* (2020) prévoit un mécanisme de coopération judiciaire à l'intérieur de l'UE. Le juge peut aussi désigner un expert chargé d'une mission à exécuter en partie dans un autre État membre, dès lors que cela n'affecte pas les prérogatives de cet État (CJUE, 21 février 2013, *ProRail*, C-332/11).

En dehors de l'Union, il faut recourir à la coopération judiciaire internationale, sur le fondement de conventions internationales existantes.

La preuve extrinsèque est imparfaite, mais peut emporter la conviction.

Elle consiste à démontrer la haute probabilité d'une IF lorsque :

- **La signification de l'acte** (paiement, consentement, acte unilatéral, contrat, testament, libéralité, etc.) **est invraisemblable**, par exemple parce qu'elle est contredite par d'autres actes ou faits, eux-mêmes prouvés ;
- **Le dommage ou l'acte litigieux ne peut s'expliquer que par une IF**, toutes les autres causes ayant été écartées.

C'est l'application de la maxime *Res ipsa loquitur*, et de l'admission des présomptions de fait fondées sur des indices graves, précis et concordants (art. 1382 du Code civil).

La Cour de justice a fait usage de ce type de preuve extrinsèque, en matière de responsabilité du fait des produits défectueux.

Ex : CJUE *Sanofi Pasteur* (2017) C 621/15

NB : En l'espèce, il s'agissait de la **responsabilité** d'un laboratoire **du fait d'un vaccin** contre l'hépatite B supposément défectueux. **Le patient avait développé une sclérose en plaques peu après la vaccination**, sans qu'existe de consensus scientifique sur un lien de causalité.

La Cour admet que le juge national se fonde sur des **indices graves, précis et concordants** : la **proximité temporelle**, **l'absence d'antécédents** personnels et familiaux, **le nombre significatif de cas répertoriés**.

En matière numérique, le raisonnement est transposable à l'IF.

La directive 2024/2853 sur la responsabilité du fait des produits défectueux, applicable aux produits mis sur le marché après le 8 décembre 2026, couvre le logiciel et organise la communication des éléments de preuve (art. 9) et des présomptions de défectuosité ou de causalité en cas de complexité technique (art. 10).

De lege ferenda, l'on pourrait concevoir un régime d'indemnisation sans preuve de l'attaque, assorti d'une obligation de cyber-assurance.

Ce régime serait concevable pour les systèmes à haut risque, lorsque l'asymétrie probatoire rend l'attaque pratiquement indémontrable.

LA RESPONSABILITÉ

Pour l'essentiel, trois responsabilités peuvent être engagées :

- La responsabilité de l'injecteur, aux plans civil et pénal ;
- La responsabilité de l'injecté, au plan civil, voire pénal, à l'égard de la victime ayant subi un dommage du fait du dysfonctionnement du système ;
- La responsabilité de l'évaluateur ou du certificateur, qui a attesté de la robustesse du système ciblé.

Ex. : un robot chirurgical victime d'une IF dysfonctionne et blesse un patient. Une responsabilité civile ou administrative de l'établissement ou du fabricant est concevable ; une responsabilité pénale, par exemple pour blessures involontaires, l'est également.

L'injecté

Plusieurs fondements de responsabilité sont concevables :

- responsabilité pour **faute** (art. 1240 du Code civil) ;
- responsabilité du fait des **produits défectueux** (art. 1245 et suivants du Code civil ; directive 2024/2853)
- responsabilité au titre du **RGPD** (art. 82) ;
- responsabilité du **prestataire de services de confiance qualifié**, présumé avoir agi intentionnellement ou par négligence (eIDAS, art. 13).

Constituent des **causes exonératoires** :

- Le risque de développement (art. 1245-10, 4° du Code civil), lorsque l'état des connaissances ne permettait pas de déceler le défaut ;
- La force majeure (par exemple, pour une attaque de niveau étatique).

La chaîne d'approvisionnement ne dilue pas l'obligation. Il n'y a pas d'épuisement de la responsabilité.

Ainsi, le *Règlement Cyber-résilience* impose au fabricant du produit final une diligence sur les composants de tiers qu'il intègre, et la directive 2024/2853 rend le fabricant d'un composant défectueux responsable aux côtés du fabricant du produit.

L'évaluateur

La responsabilité civile de l'évaluateur peut être recherchée sur le **terrain contractuel** à l'égard de son client, et **délictuel** à l'égard des tiers.

La responsabilité pénale de l'évaluateur, par exemple pour **mise en danger d'autrui** (art. 223-1 du Code pénal), peut théoriquement être engagée.

L'injecteur

Deux cas sont à distinguer :

- Celui de l'injecteur ;
- Celui du diffuseur de moyens ou de résultats d'injection.

Sur ce dernier point, deux affaires ont déjà donné lieu à des décisions relatives aux obligations du chercheur qui publie, et au pouvoir du juge de suspendre la publication.

Ainsi, au Pays-Bas, de l'affaire NXP (Rechtbank Arnhem, 18 juillet 2008, BD7578)

En l'espèce, un juge des référés refuse d'interdire la publication de l'algorithme de la carte *Mifare Classic*. Il fonde sa décision sur l'intérêt de publier ces résultats, écarte les scénarios catastrophes que l'industriel opposait, et impute le préjudice allégué non aux chercheurs qui ont révélé la faille, mais au fabricant qui a mis le produit sur le marché.

De même, en Angleterre, de l'affaire Volkswagen (High Court, 25 juin 2013, [2013] EWHC 1832 (Ch))

Dans cette décision, la *High Court* suspend la publication d'un article exposant les failles de la puce d'antidémarrage *Megamos*.

La Cour ne juge pas illicite la rétro-ingénierie, car les demandeurs admettaient eux-mêmes dans la procédure que le découpage physique de la puce était licite.

En revanche, **la Cour reproche aux chercheurs d'avoir utilisé des moyens d'origine douteuse** sans en vérifier la provenance, et d'avoir refusé tout délai ou toute coupe, ce qui conférait à leur publication un caractère irresponsable.

CONCLUSION

L'injection de fautes est mal connue en droit.

Le chercheur en IF agit dans un périmètre de licéité imprécis.

Le fabricant répond d'une obligation de moyens fondée sur l'état de l'art, dont l'appréciation est par nature incertaine en justice.

Le juge peut être trompé par un faux commis par IF.

Trois propositions peuvent être émises :

- Légaliser explicitement la recherche publique en IF, et la recherche privée en circuit clos ;
- Instituer un régime de responsabilité sans faute du fait d'une IF, assorti d'une obligation de cyber-assurance, pour les systèmes à haut risque ;
- Reconnaître dans la loi la possibilité d'une preuve extrinsèque contre le résultat d'un dispositif techniquement certifié.