L'échiquier

LA STRATÉGIE DU RENSEIGNEMENT PRIVÉ

GRAND ANGLE

Souveraineté de la donnée :
Entre désillusion et réelles possibilités

PORTRAIT D'EXPERTE IE

Tiphaine LEFRANÇOIS

DERRIÈRE L'OBJECTIF

Guide de survie en milieu interprété :
Allô maman bobo

Nouvelle rubrique

L'ATELIER DE L'ENQUÊTEUR

Zéroneurone

©L'échiquier | Création originale de l'ONARP
n°12 - Janvier 2026

www.onarp.org

SOMMAIRE

04 L'ÉDITO DES ADMINS

05 ACTU JURISPRUDENCE

Droit belge : Quand l'enquête devient une procédure

11 LA TRIBUNE INVITÉE

Krisium

15 PORTRAIT D'EXPERTE IE

Tiphaine LEFRANÇOIS

19 GRAND ANGLE

Souveraineté de la donnée : Entre désillusion et réelles possibilités

22 DERRIÈRE L'OBJECTIF

Guide de survie en milieu interprété : Allô maman bobo

25 AU DELÀ DES FRONTIÈRES

Le common law

27 L'ATELIER DE L'ENQUÊTEUR

Nouvelle rubrique

Zeroneurone

29 PARTENAIRES

©L'échiquier - Création originale de l'ONARP - n°12, janvier 2026
La stratégie du renseignement privé

INSPIRATION DE CONTENU

MEMBRES DE L'ONARP

REMERCIEMENT SPÉCIAL

TIPHAINE LEFRANÇOIS

RÉDACTEURS DANS CE NUMÉRO

ANTHONY BRUNELIÈRE
CAROLE FRÉMY
GEOFFREY PAGÈS-GALDIOLO
YANN PILPRÉ
ÉMELINE STRENTZ-ZAKHAROV
THOMAS
YPSI

RÉDACTRICE EN CHEF

CAROLE FRÉMY

FONDATEUR DE L'ONARP

OLIVIER GROLEAU

ADMINISTRATEURS DE L'ONARP

CAROLE FRÉMY
OLIVIER GROLEAU

ILLUSTRATIONS

IA / DALL-E

L'ÉDITO DES ADMINS

Nouvelle année, nouveaux défis, nouvelles perspectives : toute l'équipe vous adresse ses meilleurs vœux pour 2026. Qu'elle soit riche en projets, en réussites et en découvertes professionnelles !

Dans ce numéro, nous vous proposons un voyage au cœur des mutations qui transforment nos métiers : entre évolutions juridiques, enjeux numériques et réalités du terrain.

Cap sur la Belgique avec un décryptage de la réforme de la recherche privée, qui change profondément les règles du jeu.

La tribune invitée accueille Krisium, qui nous plonge dans la cyberattaque et la nécessité d'anticiper la crise.

Le Grand Angle vous invite à explorer un enjeu clé de notre époque : la souveraineté de la donnée, entre dépendance technologique et maîtrise stratégique.

Vous découvrirez aussi l'interview de Tiphaine LEFRANÇOIS, experte en intelligence économique, qui partage son regard et ses clés pour mieux comprendre ce domaine.

Nous franchissons ensuite les frontières avec une immersion dans le common law.

Derrière l'objectif, petit billet d'humeur : entre contraintes réglementaires, interprétations et pratiques concrètes…

Nous inaugurons cette année une nouvelle rubrique : Sortez vos clés de 12, l'atelier des enquêteurs ouvre ses portes pour vous faire découvrir des outils innovants et réellement utiles à votre exercice quotidien.

À noter : exceptionnellement, la rubrique matériel fait une pause ce mois-ci, le produit convoité ayant été victime de son succès. Son test sera donc réalisé dans le prochain numéro !

Un numéro pensé pour informer, inspirer et distraire.

Très bonne lecture à tous.

Olivier GROLEAU
Fondateur | Administrateur

Carole FRÉMY
Co-Administratrice

ACTU JURISPRUDENCE
DROIT BELGE

ANALYSE OPÉRATIONNELLE DE LA LOI BELGE DE 2024 SUR LA RECHERCHE PRIVÉE : QUAND L'ENQUÊTE DEVIENT UNE PROCÉDURE

PAR
GEOFFREY PAGÈS-GALDIOLO
(SUPERVISION : KARINE TOURNAY)

La Belgique s'est dotée en 2024 d'un nouveau cadre légal global pour l'enquête privée, qui remplace le régime antérieur de la loi du 19 juillet 1991 sur la profession de détective privé. La « Loi réglementant la recherche privée » est entrée en vigueur le 16 décembre 2024 et nos confrères belges ont dû s'y adapter ces derniers mois.

L'objectif affiché était de formaliser des obligations construites empiriquement et de mettre à niveau une profession jugée en décalage face aux exigences contemporaines de protection de la vie privée (RGPD), aux pratiques de gouvernance en entreprise et aux outils technologiques.

Dans sa version ultime, la loi de 2024 ne se contente pas de « mettre à jour » la loi de 1991 : elle déplace la logique même de l'enquête privée en Belgique, la transformant en une activité hautement normée, sous contrainte RGPD renforcée et s'inscrivant dans un raisonnement finaliste et procédural. La loi vise aussi les services internes d'entreprises qui exercent des activités de recherche privée, mais ce pan n'est pas développé dans le présent article.

1) Conséquences pratiques communes à tous les enquêteurs privés

a) Le mandat est la pièce centrale du dossier

Avant toute investigation, l'enquêteur doit disposer d'un document de mission structuré et écrit, signé du mandant et précisant : l'identité des parties (et le cas échéant, des sous-traitants), l'intérêt légitime poursuivi, la finalité exacte de la recherche, les catégories de données recherchées et la durée estimée de la mission.

Conséquence pratique : le mandat sert de clé de lecture à toute la mission (et, en pratique, à toute discussion ultérieure sur la proportionnalité des moyens mis en œuvre) et suppose dès lors une définition précise des enjeux et du périmètre de l'enquête. Exit les missions vagues, formulées de manière larges, avec les clients ne sachant pas précisément ce qu'ils recherchent.

b)Les surveillances et filatures sont drastiquement encadrées

La loi encadre « l'observation » (qu'elle définit comme le fait d'observer ou suivre une personne à son insu) par une combinaison de lieux interdits, moyens limités et durées plafonnées.

D'abord, certains lieux deviennent un no-go absolu : domicile personnel, lieux privés, et, plus largement, partout où les personnes peuvent légitimement attendre la protection de leur vie privée.

La loi prend soin de lister des exemples de tels lieux : hôtels, salles de fête privée, terrains d'une école ou d'une usine, boutiques de vêtements et toilettes.

Est aussi interdite la surveillance dans des lieux qui « par leur nature » livreraient des informations sensibles sur une personne (exemple : local syndical, lieux de culte).

Conséquence pratique : Concrètement, cela ferme la porte à toute observation « immersive » dans des espaces privés pour l'enquêteur privé.

Ensuite, la loi impose un traçage documentaire : pour chaque observation, l'enquêteur doit consigner précisément dates/heures, moyens utilisés, les lieux, l'objectif et les résultats.

Conséquence pratique : Une filature sensée être discrète est désormais doublée par une opération formaliste qui doit être auditable par des tiers (par le mandant, une autorité administrative ou encore un juge).

Une autre conséquence pour l'enquêteur est la constitution obligatoire de « dossiers d'enquêtes » par mission, qui doivent être conservés pendant 3 ans et comprenant toutes les pièces transmises par le mandant, un aperçu chronologique des actes d'investigation, un détail des moyens utilisés et leur justification, etc.

Enfin, et c'est certainement le plus impactant, la durée d'observation d'une même personne, pour la même finalité et pour le même mandant, est limitée à moins de 96 heures par mois (et toute journée entamée vaut une journée complète).

Conséquence pratique : La mission devient illégale dès que le seuil est dépassé, avec des conséquences aussi bien pour l'enquêteur que pour la procédure du mandant. Les stratégies de « preuve par répétition » deviennent périlleuses si elles reposent sur une surveillance étalée.

c)Restrictions sur les moyens techniques utilisables

Une interdiction frontale est posée par la loi de 2024 : il est interdit à l'enquêteur privé de mettre à disposition, installer, faire installer, ou utiliser des appareils (ou exploiter leurs données) en vue de déterminer les lieux où l'enquêté se trouve ou les déplacements qu'il effectue. C'est donc la fin du « tracking » de type balises/GPS.

Certains commentateurs estiment également que cette interdiction pourrait être interprétée comme étendue à tous matériels techniques de captation d'images ou de sons.

La loi prend d'ailleurs soin de préciser que seuls les appareils photos et appareils d'amélioration optique (ex : longue focale) restent autorisés.

Il existe bien une dérogation, mais celle-ci suppose le consentement préalable de la personne objet de l'enquête.

Conséquence pratique : Exit l'utilisation de différents moyens techniques pour les enquêtes dans un contexte contentieux.

d)Le rapport d'enquête final devient un déclencheur procédural

La loi encadre plus strictement le contenu du rapport : les conclusions doivent être licites et précises, les informations qu'il contient doivent être adéquates, pertinentes, et strictement limitées à ce qui est nécessaire et proportionnel au regard de la finalité légitime décrite dans le mandat.

Mais surtout, la transmission du livrable final au client devient le début d'une séquence d'obligations d'informations des personnes concernées, a fortiori lorsque le mandant décide d'en faire usage. En effet, la loi institue un mécanisme d'informations des personnes objets de l'enquête en cas de suite donnée au rapport.

Ainsi, si le client du détective souhaite faire usage du rapport, il doit l'en informer et celui-ci doit alors communiquer immédiatement et par écrit à la personne enquêtée certaines informations : identité du client, nature/objet de la mission, dates de début et de fin, existence des droits RGPD. Le mandant ne pourra faire usage du rapport que s'il est en mesure de rapporter la preuve que toutes ces étapes ont été respectées.

Conséquence pratique : Le rapport n'est plus seulement un élément probatoire, il devient, sur le fondement du RGPD, un événement procédural à anticiper. Cette situation a nécessairement des conséquences en termes de coûts et de délais, mais surtout un immense impact stratégique sur les dossiers contentieux. Par ailleurs, contacter les personnes enquêtées n'est pas toujours aisé : quid par exemple de l'adresse postale d'un amant aperçu durant une filature pour adultère, mais non identifié par l'enquêteur ou son mandant ?

2) Conséquences spécifiques pour les enquêteurs en fraude à l'assurance

La loi de 2024 précise que la gestion normale des sinistres est exclue du champ de la recherche privée tant qu'une enquête fraude n'est pas ouverte.

Conséquence pratique : Il devient crucial pour les compagnies d'assurance de documenter le point de bascule entre « gestion normale du sinistre » et « enquête pour suspicion de fraude ». A défaut, le dossier sera grandement fragilisé devant les juridictions.

Les enquêteurs d'assurance bénéficient néanmoins d'exceptions ciblées, la plus notable étant la possibilité d'enquêter sur l'état de santé d'une personne lorsque plusieurs critères sont réunis.

Ainsi, lorsque le détective est mandaté par une compagnie d'assurance et agit strictement sur instructions d'un médecin-contrôle afin de vérifier la cohérence entre l'état de santé déclaré et les activités réelles d'une personne, il est autorisé à réaliser des observations « sensibles » sur cette personne (sur son état de santé apparent et sur sa situation privée personnelle).

Le résultat de l'enquête est communiqué exclusivement au médecin-contrôle (et non pas à l'assureur).

Conséquence pratique : L'enquêteur privé ne peut plus fonctionner comme un simple « capteur » des faits transmis par le gestionnaire. Il doit désormais intégrer un circuit complexe où le médecin-contrôle devient le destinataire central de certains axes d'enquêtes, ce qui multiplie les interfaces et rigidifie le calendrier de l'enquête. Par ailleurs, la limite des 96 heures d'observation par mois impose de repenser les enquêtes de préjudices corporels : travaux préparatoires approfondis pour optimiser au mieux le temps de filature disponible. Enfin, l'enquête sur la fraude intermittente, qui reposait classiquement sur des observations longues, devient mécaniquement plus coûteuse et hasardeuse à documenter.

3) Enquêteurs généralistes : un cadre nettement plus restrictif

Pour les généralistes (contentieux civil et commercial, due diligence, enquêtes de vérifications/screening, enquêtes de solvabilité, recherches de domicile, etc) la loi de 2024 a un effet particulièrement marqué et restrictif.
Par principe, sont désormais totalement prohibées les investigations révélant directement ou indirectement : les opinions politiques ou philosophiques, les convictions religieuses, l'appartenance syndicale, l'état de santé, le comportement sexuel ou l'orientation sexuelle, l'origine ethnique, les litiges non encore jugés publiquement, les informations classifiées (habilitations de sécurité), etc.

Conséquence pratique : De nombreuses informations sur les personnes – alors même qu'elles peuvent révéler un risque, un réseau relationnel, un comportement déloyal, etc – deviennent par nature totalement inutilisables.

Le texte encadre en outre très fortement les enquêtes pré-contractuelles. Il prévoit ainsi qu'une enquête privée portant sur l'état civil, la situation familiale, financière, patrimoniale ou professionnelle, ou la moralité d'une personne, visant à vérifier « si elle peut bénéficier de la confiance du mandant afin de contracter » ne peut être débutée qu'après la réunion cumulative de deux conditions :
1-La cible a eu connaissance de l'identité du mandant, de la raison et de la nature de la recherche ;
2-La cible a donné son consentement à l'enquête.

Conséquence pratique : Cela impacte très négativement les missions de vérifications préalables/due diligence, qui, pour des raisons évidentes, reposent sur une approche discrète.
De même, pour la recherche de domicile ou de patrimoine, l'enquêteur ne peut communiquer ses conclusions à son client que s'il a obtenu le consentement écrit de la cible de l'enquête, après information quant à l'identité du mandant et l'objet de la mission. L'idée directrice reste la même : la recherche « administrative » sur une personne ne peut plus être un réflexe neutre pour l'enquêteur, mais devient un processus qui doit être consenti par la personne enquêtée.

De plus fort, la loi de 2024 interdit formellement la consultation ou l'exploitation de fichiers automatisés non accessibles au public, l'exploitation d'informations obtenues par un délit ou de façon illégitime, ou encore l'utilisation de techniques de provocation et de ruse (notamment : se faire passer pour une autre profession, **même de manière implicite).**

4) Conclusion et mise en perspective avec la France

La cohérence d'ensemble de la loi belge est assez lisible : l'objectif est de rendre l'enquête privée prouvable, traçable et contestable, en limitant les techniques intrusives et en organisant une transparence qui permet à la personne concernée d'exercer ses droits avant que le mandant du détective n'exploite l'information. La loi souffre d'angles morts et de flou juridiques, pour lesquels nos confrères belges sont en attente de décisions jurisprudentielles qui viendront clarifier le régime.

Il est évident que la loi fragilise les pratiques historiques et les acteurs isolés, et favorise par voie de conséquences les plus grosses structures, capables d'absorber la charge de conformité et de produire une traçabilité juridique irréprochable.

En France, la profession a été réglementée plus tardivement (plus de 20 ans après la loi belge de 1991) et sa la définition légale admet qu'elle consiste à recueillir des informations « même sans faire état de sa qualité ni révéler l'objet de sa mission ». Une telle définition apparait totalement incompatible avec l'esprit du législateur belge, qui a préféré ancrer la recherche privée dans une logique de transparence et de consentement.

Autrement dit, en l'état du droit positif, la France reconnait explicitement une marge de manœuvre et une part de discrétion structurelle aux enquêteurs privés, là où la réforme belge tend objectivement à la réduire.

Pour l'heure, aucune source publique ne permet d'identifier un projet visant à transposer en France un modèle comparable à la loi belge (avec plafond pour les filatures, mécanismes d'informations obligatoires des personnes visées par l'enquête, etc). La trajectoire observable est plutôt celle d'une professionnalisation et d'un renforcement accru des contrôles administratifs (CNAPS, CNIL, formations obligatoires, référentiels, harmonisation des pratiques). Espérons que le législateur français ne décide pas de changer de cap.

TRIBUNE INVITÉE

Krisium

PAR YPSI

Cyberattaque : et si ça vous arrivait demain ?

Pourquoi les professionnels de l'investigation doivent aussi s'entraîner à la crise numérique ?
Imaginez : lundi matin, vous allumez votre ordinateur. Écran noir. Vos dossiers clients, vos rapports d'enquête, vos photos, vos notes... tout est chiffré. Un message s'affiche : "Payez 50 000 € en Bitcoin ou vos données seront publiées." Que faites-vous ?

Une menace qui ne cible plus seulement les grandes entreprises

On pourrait croire que les pirates informatiques s'attaquent uniquement aux multinationales. C'est faux. Aujourd'hui, les cybercriminels ratissent large : TPE, professions libérales, artisans... et les détectives privés constituent des cibles particulièrement intéressantes.

Pourquoi ? Parce que vos dossiers valent de l'or. Informations confidentielles sur des affaires sensibles, données personnelles de vos clients, éléments de preuves... Entre de mauvaises mains, ces informations peuvent servir au chantage, à la revente, ou simplement détruire votre réputation et celle de vos clients.

Le jour où tout bascule

Nous avons tous entendu parler d'un confrère ou d'une connaissance touchée par ce type d'attaque. Le scénario est souvent le même :

-Un email piégé ouvert par mégarde
-Une clé USB trouvée et branchée par curiosité
-Un mot de passe trop simple ou réutilisé partout sans double authentification.
-Une mise à jour repoussée "à plus tard"

Et soudain, c'est le chaos. Les clients appellent, inquiets. Les dossiers en cours sont bloqués. Faut-il payer ? Prévenir la police ? Contacter un spécialiste ? Dans la panique, on prend souvent les mauvaises décisions.

S'entraîner avant d'être confronté à la réalité

C'est précisément pour éviter ces situations que la plateforme Krisium (http://www.krisium.fr) a été développée par la société YPSI. Le principe : vous plonger dans une simulation de crise cyber, en conditions réelles, pour apprendre les bons réflexes. Et sans connaissance technique préalable.

Concrètement, pendant quelques heures, vous vivez une attaque fictive. Un animateur joue le rôle des "méchants" et fait évoluer le scénario selon vos réactions. Vous devez prendre des décisions : isoler votre poste ? Appeler votre prestataire informatique ? Prévenir vos clients ? Déposer plainte ?

L'objectif n'est pas de devenir un expert en informatique, mais de savoir comment réagir, qui appeler, et dans quel ordre. Exactement comme un exercice incendie vous apprend à évacuer un bâtiment sans avoir besoin de savoir manier une lance à eau.

Ce que révèle un exercice de crise

Les professionnels qui ont testé ce type d'entraînement en ressortent souvent avec des révélations surprenantes :

"Je n'avais pas le numéro de mon prestataire informatique ailleurs que dans mon ordinateur..."
"Personne dans l'équipe ne savait qui devait prendre les décisions en cas de crise."
"Nos sauvegardes ? On pensait qu'elles fonctionnaient et que notre prestataire s'en occupait..."

Ces découvertes, mieux vaut les faire pendant un exercice que le jour où l'attaque est réelle.

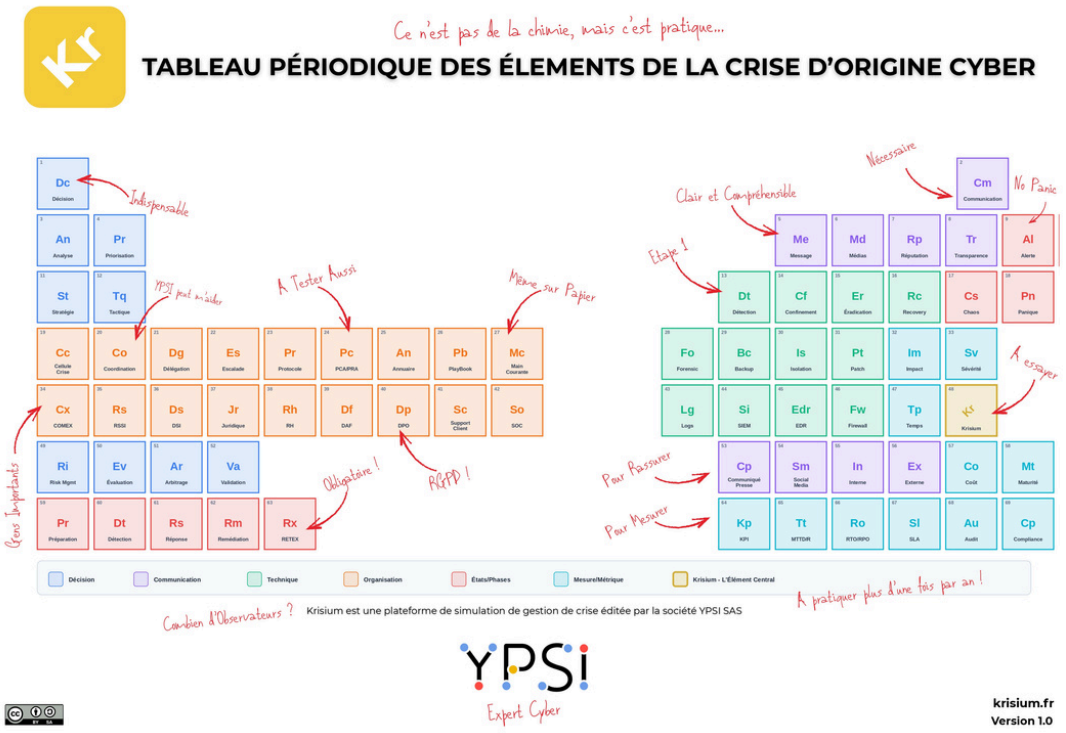
Les réflexes qui peuvent tout changer
Sans entrer dans la technique, voici ce qu'un entraînement permet d'ancrer :

- Garder son calme — La panique est votre pire ennemie
- Ne pas toucher à tout — Certains gestes aggravent la situation ou détruisent des preuves
- Savoir qui appeler — Et avoir ces numéros accessibles hors de votre système informatique
- Documenter ce qui se passe — Photos, notes manuscrites, chronologie des événements
- Protéger vos clients — Les prévenir au bon moment, ni trop tôt, ni trop tard

Un investissement pour votre tranquillité
En tant que professionnel de l'investigation, vous savez mieux que quiconque que la préparation fait la différence entre une affaire qui aboutit et une impasse.

Face aux menaces numériques, c'est la même logique : ceux qui se sont entraînés traversent la crise. Les autres la subissent.

Krisium est une plateforme d'exercice de crise cyber développée par la société YPSI. Pour organiser une session adaptée aux professionnels de l'investigation privée : contact@ypsi.fr



Quelques chiffres à garder en tête

- 1 entreprise sur 2 de moins de 50 salariés a déjà été ciblée par une cyberattaque ;
- 4 heures : c'est le temps dont vous disposez pour limiter les dégâts ;
- Les numéros utiles à avoir sur papier : prestataire informatique, banque, assurance, 17Cyber ;
- 80% des attaques exploitent une erreur humaine, pas une faille technique.

PORTRAIT D'EXPERTE IE

TIPHAINE LEFRANÇOIS

Responsable du Département Intelligence Économique
Groupe Amarante International

ONARP : Quelle fonction occupes-tu chez Amarante International ?

TL : Je suis responsable du Département Intelligence Economique chez Amarante International. Amarante est une société de sécurité globale qui opère à l'international ; j'y travaille depuis bientôt 3 ans.

ONARP : Quelles sont tes missions concrètes ?

TL : Les missions de ce poste sont multiples, je suis à la fois à la production, au management, ainsi qu'au développement commercial.

ONARP : On a parfois le sentiment que l'IE recouvre de nombreuses définitions. Quelle est la tienne ?

TL : C'est très large. Mais, pour moi l'IE, c'est du renseignement d'affaires. Quand on dit intelligence économique, c'est ça. Finalement, les ARP qui travaillent sur des thématiques commerciales tombent dans cette définition, même si les prérogatives diffèrent.

ONARP : Que te demande t-on comme "renseignements" ?

TL : Je réalise des investigations sur des personnes des sociétés, des secteurs et technologies. En général, je travaille sur une base de droit de la compliance : lutte contre la corruption, lutte contre la fraude, le détournement d'argent ou de marchandises. Tout ce qui a trait à la fraude ou aux suspicions. Je réalise des enquêtes internes ou externes.
Nos enquêtes se font en OSINT, qu'on appelle souvent études de due diligence, dans le cadre de fusion acquisition par exemple. On vérifie que les données financières sont accessibles, c'est une analyse global. Le rapport final est une sorte de document d'informations analysées accessibles en open source, ainsi qu'une cartographie des risques, qu'ils soient économiques ou réputationnels ou tout autre. Cela permet à nos clients d'avoir une vision 360 avant de prendre une décision, peu importe le projet.

ONARP : As-tu des prérogatives particulières ?

TL : Non. En revanche, on utilise des plateformes qui sont des agrégateurs de données.

ONARP : Cela pré-mâche le travail ?

TL : Non, tu dois faire l'analyse par toi-même. Les données doivent être lues et étudiées pour en sortir une analyse juste. La plus-value, c'est que nous lisons entre les lignes, entre les chiffres, la structure, les employés, la réputation. Le scoring final va permettre au client de savoir quoi penser de la société ou la personne avec laquelle il veut entreprendre.

ONARP : Sans données financières publiques, comment fais-tu ?

TL : On cherche des moyens de les trouver ou de trouver des signaux faibles, puis on va travailler alors sur la partie plus réputationnelle. Sur le niveau 3 des dues diligences, nous faisons appel à des sources HUMINT pour confirmer ou infirmer des informations. On peut faire appel à des ARP pour réaliser des enquêtes de terrain pour répondre à certaines questions. En amont de cela, nous réalisons la partie OSINT nous-mêmes. Nous ne pouvons pas réaliser de surveillances ou de filatures dans le cadre de nos dossiers. J'ai eu par le passé cette casquette ARP, et j'essaie de démocratiser ces solutions lorsqu'elles peuvent être utiles à nos clients. Ils n'y pensent pas toujours, mon parcours me permet de dire si c'est faisable et judicieux.

ONARP : Les dossiers à traiter sont-ils variés ?

TL : Les problématiques sont diverses. 75% a 80% des enquêtes sont à l'international : Afrique, Amérique latine, Europe de l'est… Les cas, les fraudes sont multiples, les gens sont créatifs ! Dans mon groupe, nous avons 28 filiales dans le monde, ce qui nous offre un réseau capital pour opérer partout dans le monde.

ONARP : Combien traites-tu de dossier en un mois ?

TL : Parfois, un seul qui peut durer des mois, en parallèle des autres. Parfois, ils sont plus petits, cela peut varier de 5 à 20 dossiers ! Je ne travaille pas seule dessus, notre équipe est un mélange de compétences. Par exemple, moi, je suis une pure osinteuse, mon équipier excelle dans la veille ; j'ai un autre analyste spécialisé en cyber. Nous avons un pôle géopolitique également, où les membres peuvent nous informer en temps réel de tout ce qui se passe sur une zone du monde, c'est une énorme plus-value au quotidien dans nos missions. C'est d'ailleurs grâce à ces synergies que nos analyses sont réputées sur le marché.

ONARP : Quel est le droit qui t'encadre ?

TL : Le droit commun, comme tout le monde, celui de la compliance dans nos études.
Nous respectons scrupuleusement les règles.

L'IE n'est pas encadré comme les ARP, mais nous œuvrons dans les limites du droit commun et de l'éthique. Des commissions sont en cours pour savoir s'il faut instaurer un cadre spécifique, mais à mon sens, l'intelligence économique ne nécessite pas cet encadrement qui risque de nous retirer des accès publics alors que notre accompagnement est primordial pour l'économie et la compétitivité des entreprises. Je trouve que dans ce secteur, il n'y a pas de débordement, les acteurs ne font pas n'importe quoi. Il ne s'agit pas d'espionnage industriel.

ONARP : Les clients sont-ils tous des grandes entreprises ?

TL : Non, nous avons des TPE/PME que l'on accompagne avec plaisir. Ils recherchent en général des analyses de marché parce qu'ils veulent grossir. Nous allons les aider à s'implanter, à trouver les meilleurs partenaires et ressources pour se développer. Nous faisons appel à des experts quand cela peut être utile et que le sujet est spécifique. Pendant des mois, j'ai pu m'avaler des rapports énormes sur des sujets inconnus, pour comprendre et avoir une idée claire de mes sujets. Dans l'IE, on passe du coq à l'âne, c'est ça qui est génial ! Il y a une détermination absolue à tout trouver sur le sujet donné pour accompagner au mieux nos clients.

ONARP : Combien coûte une enquête réputationnelle ?

TL : Il y a différents niveaux.
De niveau 1, c'est un check basique qui répond à des normes de compliance simple.
De niveau 2, les investigations sont plus poussées, et on identifiera tout ce qui se trouve en sources ouvertes et les risques qui vont avec.
Les études de niveau 3, il y aura en plus du reste, des auditions et entretiens. Pour chaque étude, une enquête préliminaire est réalisée pour pouvoir estimer le cout de la prestation : cela varie énormément, par exemple, le cout entre une enquête sur une PME et sur une multinationale ne sera jamais la même.

"Ils réalisent (les clients) qu'internet n'oublie jamais."

Les process sont normalisés. En droit de la compliance, les recherches à faire sont en fonction du projet du client et des risques selon le secteur géographique, la profession impliquée etc. C'est cela qui va déterminer le niveau de l'étude dans le but de ne pas être intrusif. Les dues diligences doivent rester raisonnables, conformément à la jurisprudence.
Les entreprises savent qu'on ne peut pas faire n'importe quoi et d'ailleurs, ne demandent pas des choses délirantes. Ils connaissent les risques et sont très attentifs à leurs demandes. Nous n'avons pas à les recadrer en règle générale.

ONARP : Y'a t-il des particuliers dans ta clientèle ?

TL : Ce n'est pas la majorité, mais nous en avons. Par exemple, un particulier fortuné dans le secteur de la cryptomonnaie, qui va vouloir gérer ses risques d'extorsions ou de kidnapping peut nous demander une enquête sur lui-même pour contrer les menaces. Il va nous demander de se mettre à la place d'un éventuel attaquant pour comprendre comment il pourrait être localisé ou ce qui circule sur lui qui pourrait le mettre en danger.
Il s'agit pour eux de se prémunir, ce sont des audits de vulnérabilité et à partir de là, ils nous autorisent à tout rechercher. Ils réalisent qu'Internet n'oublie jamais. En tapant un nom un prénom sur internet, effectivement ça ne va pas réapparaître, mais pour quelqu'un qui s'y connaît un peu, tout réapparaît. Certaines sociétés par exemple, qui voudraient effacer le passage d'un collaborateur, même si le nom n'est apparu qu'une semaine, on le saura. Toutes les solutions OSINT misent bout à bout permettent des recherches complètes.

ONARP : Pratiques-tu l'OSINT en dehors du Groupe Amarante ?

TL : Oui, je suis réserviste au COMCYBER-MI de la gendarmerie en qualité de spécialiste OSINT. En France, nous sommes environ 70.

PROPOS RECCUEILLIS PAR CAROLE FRÉMY

GRAND ANGLE

SOUVERAINETÉ DE LA DONNÉE : ENTRE DÉSILLUSION ET RÉELLES POSSIBILITÉS

De nos jours, quel ARP, analyste OSINT ou expert IE ne s'est pas posé cette question " Comment stocker mes données ?", Un dilemme complexe aux regards de problématiques de souveraineté exacerbées par les différents conflits actuels, qu'ils soient économiques, politiques ou armés.
Les affaires traitées par un ARP, même si celle-ci reste en France, peuvent parfois avoir un lien avec des entreprises ou des clients de nationalité différente. Or il est parfois nécessaire d'avoir accès, de collecter, de traiter, d'analyser et de restituer des données. Mais comment les stocker alors ? Une fois ces données traitées, elles doivent être stockées de façon à éviter toute altération avant leur transmission ou pour simple archive. Les offres de services des GAFAM et autres fournisseurs nous proposent une variété de choix. La plupart penseront SharePoint, inclus dans les produits Microsoft ou à Google drive pour Google et encore à iCloud pour Apple. Néanmoins, ces solutions conviennent-elles aux affaires traitées ?

I.La souveraineté numérique

L'usage massif de solutions américaines relève simplement d'un constat. Elles sont performantes, intégrées, connues, interopérables et peu coûteuses à l'entrée. C'est précisément cette évidence fonctionnelle qui masque leurs implications juridiques et stratégiques.

Pour rappel, ce que dit le Cloud Act de 2018 : " Le CLOUD Act (Clarifying Lawful Overseas Use of Data Act) est une loi américaine de 2018 permettant aux autorités américaines d'exiger l'accès aux données électroniques détenues par des entreprises américaines, même si ces données sont stockées à l'étranger (hors des États-Unis), dans le cadre d'enquêtes criminelles ou de sécurité nationale, créant ainsi un conflit de souveraineté avec des réglementations comme le RGPD européen. Cette loi prime sur le lieu de stockage et contraint les fournisseurs de services cloud américains (Google, Microsoft, Amazon…) à fournir les données sous contrôle, qu'elles soient sur des serveurs aux USA ou en Europe".

Ce sujet est de plus en plus préoccupant compte tenu des enjeux géopolitiques actuels et avec la création d'un « cloud souverain européen » géré par…Amazon, un acteur américain. L'enjeu derrière ce projet de plus de 7 milliards d'euros, n'est pas technique mais juridique. Ici, le cloud act prévaudra toujours. Par conséquent, la proposition d'une alternative d'un cloud souverain géré par un américain n'est toujours pas une option envisageable. La souveraineté ne se délègue pas par contrat lorsque la loi applicable est extraterritoriale.

II. Des usages avec des degrés de risques différents

Une fois le cadre juridique posé, la question n'est plus de savoir quelle solution est "bonne" ou "mauvaise", mais à quels usages correspondent quels niveaux de risques acceptables.

Dans ce cas de figure, les solutions classiques sont-elles adaptées à l'activité ? La question se posera également sur des solutions grand public de transfert de données, type Dropbox, WeTransfer et autres. Prendre en compte ces problématiques permettra d'anticiper des requêtes potentielles dans le cas d'affaires internationales ou incluant des clients étrangers.
Il en va de même sur la sûreté de ses données qui "obligent" également à un stockage qui évite toute altération de ces données. Dans ce cas, il sera nécessaire de choisir la solution qui offre les meilleures garanties de ce point de vue également. Des solutions européennes et françaises existent mais moins connues que leurs concurrentes mondiales. Prenons l'exemple de WIMI, une solution française payante qui propose une alternative aux suites habituellement utilisées. Un espace de stockage est également proposé dans l'abonnement, ce qui permet de conserver ses données dans l'espace européen. Autre solution possible, celle de LockSelf qui propose plusieurs services cloud, dont celui de stockage et de transferts de données.

Pour certains, il est également possible d'utiliser un simple abonnement Proton incluant stockage de confiance et simplicité d'utilisation. Pour les plus techniques, un serveur personnel hébergé en local de type NAS est aussi la solution pour une maitrise quasi totale de ses données, de son stockage et de ses sauvegardes.
Le but n'est pas de critiquer ou stigmatiser une solution plus qu'une autre, mais de permettre un éveil de conscience dans le cadre des activités d'un ARP qui sera de plus en plus confronté au changement de paradigme du monde et des puissances actuelles à des obligations. Les législations en termes de propriété de données sont de plus en plus complexes, l'intégration de l'IA y ajoute encore une couche de complexité. Choisir de stocker ses données dans l'espace européen voire même en France (souveraineté des données) permet de se préparer ou de se prémunir à de futurs recours judiciaires contre les stockages de cette même donnée dans les espaces choisis.

Traiter ces sujets n'est pas chose simple en plus de la charge de l'activité, mais elle doit être prise en compte pour définir une stratégie claire qui permettra également une réduction de coûts d'exploitation potentielle et substantielle.

Le dernier point à aborder, et non des moindres, est le changement des habitudes. La faille principale n'est pas technologique mais comportementale. Les pratiques individuelles (smartphones, automatisations, partage instantané) court-circuitent souvent les politiques de sécurité les mieux pensées. Sommes-nous prêts à changer nos habitudes qui permettent d'enregistrer les photos et documents reçus directement sur le Cloud du smartphone, ou de transférer un fichier à un client sans prendre le temps d'utiliser une plateforme qui aura un meilleur niveau de protection que celle utilisée pour transférer des photos "classiques" ?

Pour conclure

Ainsi, lorsque des données peu stratégiques sont manipulées, les outils grand public restent acceptables. Quand ce sont des données opérationnelles internes, des solutions européennes sont recommandées. En revanche, pour des données très sensibles; transnationales, alors le stockage souverain ou maîtrisé directement (NAS, chiffrement avec clés exclusives) sont indispensables.

La souveraineté des données et du numérique n'est pas un sprint mais un marathon où chaque pas, chaque décision, chaque transfert expose ou sécurise les clients.

Pour l'ARP, l'analyste OSINT ou l'expert en intelligence économique, la question n'est pas de viser une souveraineté absolue, souvent illusoire, mais de savoir où se situent ses lignes rouges : quelles données ne doivent jamais sortir d'un cadre juridique maîtrisé, quels usages peuvent tolérer un risque résiduel, et quelles dépendances sont acceptables.

La souveraineté numérique n'est donc pas une fin en soi, mais un processus continu de lucidité stratégique.

POUR ALLER PLUS LOIN :

https://www.wimi-teamwork.com/fr/
https://www.lockself.com/
https://www.boulanger.com/aide/glossaire/definition-nas

PAR ÉMELINE STRENTZ-ZAKHAROV & THOMAS

DERRIÈRE L'OBJECTIF

GUIDE DE SURVIE EN MILIEU INTERPRÉTÉ : ALLÔ MAMAN BOBO

L'idée était bonne. Elle l'est toujours, sur le papier.
Contrôler une profession sensible, rappeler un cadre, prévenir les dérives, assurer la sécurité du public comme celle des professionnels : difficile de s'y opposer sans mauvaise foi. Qui, honnêtement, irait contester la légitimité d'un tel encadrement quand il se présente comme un gage de sérieux et de protection ?
Le grand public ignore largement qui nous gouverne. Il nous imagine parfois électrons libres, évoluant hors de tout cadre. Que nenni. Nous avons une autorité depuis 2012, un père : le CNAPS. Sous la tutelle de l'État, il lui revient de nous guider dans le dédale des règles, d'accorder nos agréments et, à la tombée du jour, de franchir le seuil de notre chambre pour en scruter l'ordre. Pourtant, aux premiers pas de notre parcours, sa présence se fait rare, presque fantomatique.

Dans les écoles privées dont beaucoup sont issus - moi la première - et où nous avons longuement tété le sein du savoir réglementaire, les premières recommandations nous sont servies très tôt. Chaque formateur y va de ses anecdotes, pas toujours adossées à un texte précis, pour expliquer que ceci est possible, que cela ne l'est pas. Dont acte. Nourrissons que nous sommes, incapables encore de distinguer la bonne dose de lait de l'excès, nous absorbons docilement. Et si d'aventure nous régurgitons, nous ravalons aussitôt. Gloup !

Puis nous grandissons au milieu des nôtres. Et là encore, les discours se multiplient. Conseils fragmentés, recommandations contradictoires, certitudes affirmées sans toujours plus d'appui juridique. Comme un réflexe humain, nous nous raccrochons à la loi du nombre : plus une recommandation circule, plus elle doit être juste. Sans texte clairement identifié - parfois difficile à dénicher - nous appliquons ce qui se pratique à bas bruit, convaincus que la répétition finit par faire norme : erreur enfantine confondante.

Le père n'a rien d'un génie : sa science jaillit des pages du Code de la sécurité intérieure (CSI), qu'il plie parfois à sa propre lecture. Alors, parallèlement, et puisque nous ne sommes plus tout à fait des bébés au cerveau mou, nous lisons, nous nous informons, nous nous formons. Nous tentons de comprendre les textes qui nous encadrent : leur esprit, leur portée et leur application concrète. Les plus audacieux - ou les plus fous - vont même jusqu'à en chercher le sens tant il faut reconnaître que certains passages relèvent de la gastronomie technocratique trop épicée pour être digeste, quand elle ne se pare pas, en plus, d'un raffinement superflu.

Faute d'Ordre professionnel pour trancher la poire en deux, et dans l'impossibilité de joindre notre autorité par téléphone, nous écrivons. Des mails. Une avalanche de mails. Nous y livrons nos doutes et nos questions, craignant de le décevoir par des initiatives malheureuses. Mais le père fonctionne par délégation territoriale d'humeur changeante, il n'est donc pas exclu qu'il vous réponde oui à Bordeaux et non à Paris. Ou l'inverse, les soirs de pleine lune. Pourquoi ? Envoyez-lui un mail.

Nous traversons ainsi nos carrières de recommandations en recommandations, de mails en mails, de syndicats en syndicat… Jusqu'au jour où le père débarque en personne. Contrôle de l'activité, permis de conduire, carte grise, bref, vous connaissez la musique. On ne sait jamais s'il en demande trop, ou pas assez. S'il est fondé à exiger ceci ou cela. D'une délégation territoriale à l'autre, l'absence d'un document pourra constituer un manquement grave… ou être anecdotique. Rien n'est pleinement harmonisé, de l'aveu même de ceux qui en reviennent avec quelques rougeurs persistantes sur le postérieur. Il arrive que le père frappe dur, sans retenue, fidèle à une évidence dont il paraît l'unique gardien.

Le bébé que nous avons été a bel et bien grandi. Il est aujourd'hui autonome, formé, agréé et réputé en règle, sous réserve d'interprétation. Il exerce avec une conscience professionnelle qu'il s'efforce de maintenir irréprochable. Son livre préféré n'est plus un recueil à colorier, mais le Code de la sécurité intérieure qu'il feuillette pour tenter de trouver le sommeil. Coincé entre une pratique de terrain dont la légitimité se mesure à coup de jurisprudence et une réglementation administrative instable, inventive jusqu'à l'absurde, le repos se fait rare. On s'endort tard, on se réveille maussade. On a cru, l'espace d'un instant, pouvoir souffler lorsque le père CNAPS a livré son référentiel. Des mois de chantier et l'on s'imaginait déjà un édifice abouti : la quintessence du CSI, enfin capable de servir de diapason aux contrôleurs. Déception. Annoncée en pierre de taille, la bâtisse se révéla n'être qu'un amas de cartons aux couleurs empruntées à des matériaux nobles.

Mais le père ne manque pas d'idées. Dans sa besace, un nouveau projet : un bâtiment plus vaste, plus massif, plus majestueux encore, promis à s'élever bientôt. Et, comme souvent en matière administrative, on promeut le nom avant d'avoir éprouvé le concept et sa fiabilité : il s'appellera "Ultimate". L'histoire nous dira combien d'hivers il traversera.

Pour une profession dont la mission est précisément de maîtriser le risque, de protéger les intérêts des particuliers comme des entreprises et de colmater les failles, il est pour le moins paradoxal de la maintenir dans une instabilité chronique quant à sa propre conformité. À force d'empiler des cadres dissonants et de multiplier des contrôles opaques opérés par des délégations sensibles aux caprices de l'humeur comme à ceux du ciel ; on engendre moins de la sécurité qu'un climat de défiance propice aux stratégies d'évitement.

L'ironie veut que ceux qui exercent sans droit ni titre restent hors de portée de la main paternelle. Sans autorisation initiale, ou une fois celle-ci expirée, son pouvoir s'évapore. Ne jamais avoir sollicité d'agrément devient alors plus protecteur que d'en être titulaire.

Dis papa : était-ce vraiment cela, le dessein originel ?

PAR CAROLE FRÉMY

AU-DELÀ DES FRONTIÈRES

LE "COMMON LAW"

Le droit français, que nous connaissons tous, est régi par un système que l'on appelle "droit civil" ou encore "napoléonien" - car c'est bien ce dernier qui a créé le code civil -. Notre système est issu du droit romain, droit déjà très complexe pour son époque qui a, par la suite, été influencé par les règles canoniques de l'Eglise catholique et la philosophie des Lumières sans oublier la pensée impériale napoléonienne. Notre droit positif (=le droit applicable) est un droit majoritairement rédigé. Autrement dit, la France applique le droit écrit et écrit le droit qu'elle souhaite appliquer. Ça vous parait logique? Eh bien ce n'est pas le cas partout.

Bienvenue dans cette présentation non exhaustive et schématique du système anglo-saxon, communément appelé 'The Common Law'.

Source : Wikipédia

Dans cet article, nous ne parlerons que de droit civil et de common law, applicables à environ 95% des personnes dans le monde, bien que d'autres systèmes existent comme le démontre la carte ci-dessus.
Comme je vous le disais, le droit civil français est issu d'une tradition catholique vieille de plusieurs siècles. Ainsi, notre système est catégorisé comme "inquisitoire" car c'est le juge qui a le rôle principal tant dans l'aspect cérémonial des séances que dans le processus en lui-même.

En effet, c'est le juge qui établit les faits du dossier et qui applique la loi. Le procureur a pour rôle de représenter la société et ses intérêts et qui donc argumente pour faire valoir ce qui est le mieux pour la société. L'investigation est publique, régalienne, menée par les forces de l'ordre sous la direction du parquet, représenté donc par le procureur de la République. Les avocats eux, conseillent et défendent les intérêts de leurs clients en répondant aux arguments du procureur qu'il obtient grâce à l'enquête publique. Il convient toutefois de préciser qu'en matière civile, la procédure française est déjà largement contradictoire, le juge y tenant davantage un rôle d'arbitre.

La common law est issue du droit anglais, avec l'empire britannique, le système anglais s'est alors largement diffusé dans le monde. En common law, c'est la "règle du précédent" qui s'applique. Cela signifie que les décisions prises par les juges sont basées sur les décisions précédentes sur des cas similaires. La jurisprudence n'a donc pas simplement un intérêt consultatif mais est surtout le centre névralgique du droit applicable. Ainsi, le droit issu de ce système anglo-saxon est historiquement très peu codifié bien que la justice moderne ait fait apparaître de nombreuses 'Statutes' (lois votées par le parlement). Aux Etats-Unis on trouve notamment les textes constitutionnels (dont les fameux Amendments) qui posent les lignes rouges que le juge ne peut pas outrepasser. Les textes, souvent des décrets ou des décisions, sont surtout organisationnels ou des programmations administratives car c'est le juge qui prend les décisions, basées sur la jurisprudence.
Lors d'un jugement, c'est le système accusatoire qui s'applique en common law. Ce sont les avocats de chaque partie qui vont accuser la partie adverse et prouver qu'ils ont tort. On comprend alors que l'avocat anglo-saxon se doit d'avoir en sa possession les preuves. C'est pourquoi le système de preuve y est bien plus privé qu'en France. L'avocat a un droit de rassembler des preuves plus large qu'en France et fait beaucoup plus appel au détective privé qu'en France car c'est lui qui doit apporter les preuves contre la partie adverse pour convaincre le juge. Tandis qu'en France, l'avocat doit rassembler les preuves de son client, ce qui est beaucoup plus simple de par la relation qui existe entre le justiciable et son conseil.

Il me semble alors que le droit français est plus démocratique que dans le système anglo-saxon puisque la loi appliquée est celle votée par les représentants du peuple. Le droit anglo-saxon est lui beaucoup plus traditionnel voire coutumier de par sa base prétorienne. Il est intéressant de noter, et donc de comprendre un peu mieux, que dans la plupart de ces pays, notamment aux Etats-unis, les juges sont élus afin de légitimer par la démocratie les décisions de justice.
Deux traditions différentes, donc, mais un même objectif : dire le droit et rendre la justice.

PAR ANTHONY BRENELIÈRE

L'ATELIER DE L'ENQUÊTEUR

Un outil d'investigation visuel, open source et collaboratif

Zeroneurone est un outil de structuration d'enquêtes développé par Yann Pilpré, co-fondateur d'Oscar Zulu et intervenant pour le DU OSINT à l'UTT de Troyes.

Il permet de poser des éléments (personnes, sociétés, véhicules, comptes, documents...), de les relier, de les annoter, et de visualiser l'ensemble sous différentes formes.

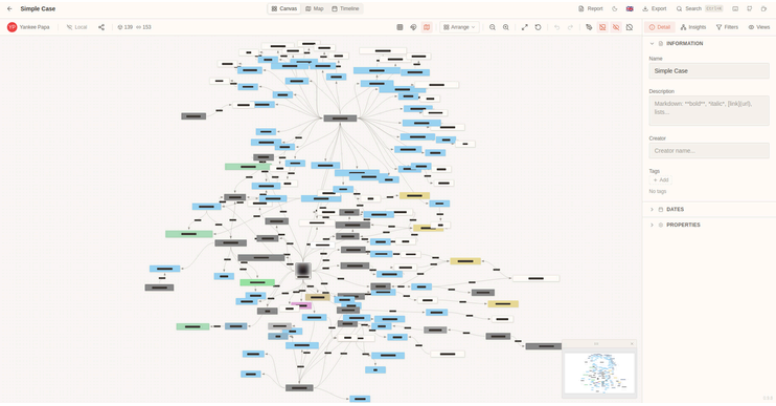
Ce que fait l'outil :

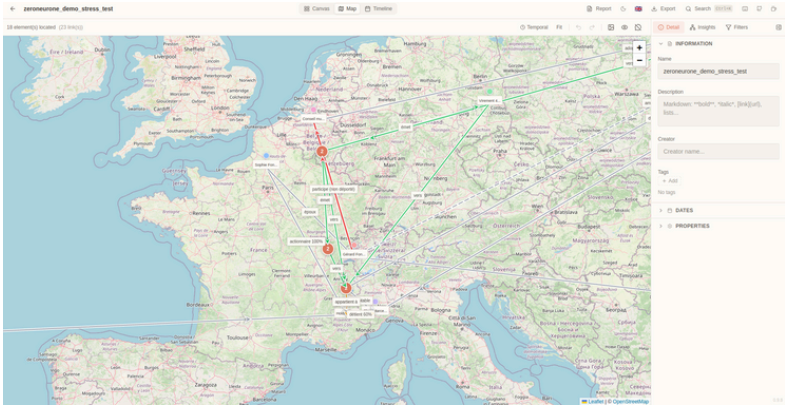
- Un canvas pour créer des éléments et des liens entre eux
- Des tags libres : vous définissez vos propres catégories (Personne, Entreprise, Véhicule, Compte bancaire...) avec les propriétés qui vont avec
- Des pièces jointes sur chaque élément : PDF, images, documents sources
- Extraction automatique des métadonnées EXIF à l'import d'une image
- Trois vues sur les mêmes données : graphe relationnel, carte géographique, timeline
- Détection de clusters : l'outil identifie les groupes de nœuds fortement connectés entre eux
- Export SVG pour intégration dans les rapports
- Notes libres directement sur le canvas
- Support des langues FR, EN, ES et DE.

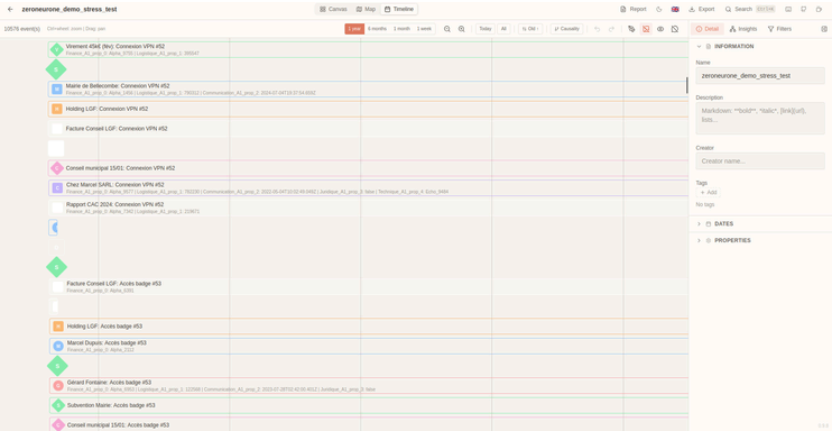
Plusieurs enquêteurs peuvent travailler sur le même dossier en temps réel. Le serveur ne fait que mettre en relation les participants, il ne stocke aucune donnée. Chacun conserve sa copie locale. L'outil fonctionne en local par défaut et vos données ne quittent pas votre machine sauf si vous décidez de les partager.

On peut importer des fichiers OSINTracker et PredictaGraph pour ceux qui utilisent déjà ces outils. Il a été conçu pour gérer sans ralentissement des enquêtes jusqu'à 1000 éléments et liens (et quelques centaines de propriétés).

Enfin il est gratuit et open source.
L'outil est accessible sur : https://zeroneurone.com
Contact : yann.pilpre@ypsi.fr







PAR YANN PILPRÉ

Partenaire OSINTER historique, testez vos compétences avec le gros pachiderme !

Enquêtez bénévolement aux côtés de cette association de lutte contre la pédocriminalité.

Partenaire d'outils OSINT proposant de la recherche, de l'analyse et de l'extraction.

Fournisseur de matériels d'investigation.

Le mind- mapping conçu pour accompagner vos enquêtes.

Partenaire d'outils de cartographie orienté GEOINT.

À NOS CÔTÉS !

Contactez-nous facilement !

contact@onarp.org

ONARP - Organisation Nationale
des Acteurs du Renseignement Privé

onarp.org

Olivier GROLEAU : Administrateur et fondateur
Carole FRÉMY : Co administratrice

©L'échiquier - Création originale de l'ONARP - n°12 janvier 2026
La stratégie du renseignement privé