



L'IA: Quelle éthique ? Quelles perspectives de société ?



MARIE AZEVEDO
PRÉSIDENTE DE L'ASSOCIATION RESOCLUB EFPA



GÉNÉRAL MARC BOGET
PRÉSIDENT D'HONNEUR DU 8E FORUM EUROPÉEN



BÉATRICE BRUGÈRE
INVITÉE D'HONNEUR DU 8E FORUM EUROPÉEN



Tables rondes animées par Alexandra BARBERIS

Avocate spécialisée en tech et digital - LEX AVOCAT
Vice-Présidente - CLUSIR PACA

Le mot de Marie AZEVEDO

Présidente de RESOCLUB EFP
Discours d'ouverture de Marie AZEVEDO



Madame Azevedo remerciait les participants au 8e forum européen de Resoclub en leur souhaitant la bienvenue. Elle rappelait le principal objectif de ce forum : cerner le rôle de l'intelligence artificielle (IA) dans le domaine de l'innovation informatique. La tendance à qualifier de 'IA' les technologies non abouties, perd de son intérêt lorsqu'elles deviennent des 'programmes' une fois parvenues à un fonctionnement efficace. Ainsi se trouve mis en lumière une certaine lenteur dans le développement de l'IA comme partie intégrante de notre progrès technologique.

Elle abordait ensuite la réalité du risque de déshumanisation que représente l'intelligence numérique et cybernétique. L'exemple du programme robot de Microsoft de 2016, adoptant des discours haineux, illustre clairement ce danger. Marie AZEVEDO partageait sa conviction selon laquelle l'IA a un rôle indispensable à jouer, notamment dans la lutte contre la fraude identitaire et la sécurisation des systèmes d'authentification.

“En somme, derrière les opportunités offertes par l'IA, je reste consciente des défis éthiques et techniques qu'elle implique. Les fraudes, le blanchiment d'argent, le financement du terrorisme, et les transactions suspectes sont des réalités auxquelles nous faisons face quotidiennement. L'IA, avec ses algorithmes d'apprentissage automatique, est une alliée précieuse pour identifier et contrer ces menaces.”

RESOCOM a développé, au cours de nos 25 années d'expérience, une big data spécialisée dans la détection des anomalies documentaires. L'identification de comportements anormaux via l'IA, sont essentiels à notre compréhension du phénomène frauduleux, tout comme les schémas de connexion incohérents ou des tentatives répétées d'accès non autorisées, pour renforcer encore notre système de sécurité.

L'IA ouvre également des possibilités prometteuses dans le domaine biométrique. Les reconnaissances d'iris, de voix, faciale et gestuelle sont des moyens innovants pour enrichir la performance d'identification. Cependant, ces avancées doivent être accompagnées d'une vigilance accrue concernant la sécurisation et l'exploitation des données personnelles. Les défis ne manquent pas : précision des systèmes face aux variations physiques dues à l'âge, respect de la vie privée, et protection de l'intimité numérique sont autant de sujets à considérer avec soin.

Le Général Marc BOGET soulignait l'importance cruciale de l'intelligence artificielle (IA) dans la lutte moderne contre la fraude. Mettant l'accent sur la sophistication croissante des pratiques de fraudes, notamment l'arnaque au président, il analysait l'efficacité de l'IA dans la commission d'escroqueries, par exemple en reproduisant des voix pour des appels plus convaincants. Le Général BOGET discutait des défis posés par la cybercriminalité, en soulignant l'utilisation professionnelle de l'IA par les cybercriminels dans des activités telles que les “rançongiciels” et le phishing sophistiqué.

Le Général BOGET concluait son propos en exprimant sa vision à la fois optimiste et prudente pour l'avenir de l'IA, reconnaissant son potentiel énorme tout en appelant à la vigilance face aux risques associés. Son discours a mis ainsi en exergue la nécessité d'une approche équilibrée dans l'adoption de l'IA, considérant à la fois ses bénéfices et ses défis.

Au sein de la gendarmerie, il expliquait comment l'IA est utilisée de manière proactive pour anticiper et contrer ces menaces. Pour autant, il mettait en lumière les défis éthiques et de sécurité liés à l'IA, notamment en termes de protection des données personnelles, et insistait sur la nécessité d'une utilisation responsable de cette technologie.

Général Marc BOGET

Président d'honneur,
Directeur de la stratégie digitale et technologique
GENDARMERIE NATIONALE



INNOVATION ET INTELLIGENCE ARTIFICIELLE : APPROCHE ET PERSPECTIVES

L'Intelligence Artificielle va être au cœur des usages incontournables de notre société. L'importance de ses capacités de développement va engendrer des risques inhérents à celle-ci, par rapport à la capacité de réaction de l'humain. Une technologie allant très vite et très loin face à l'incapacité de contrôle simultané de ces nouveaux usages, pourrait être un facteur de vulnérabilité pour nos sociétés susceptibles de devenir des cibles.



Dans un contexte où la cybercriminalité et l'usurpation d'identité représentent des défis majeurs, la table ronde a exploré les possibilités et les limites de l'intelligence artificielle (IA) dans la lutte contre ces phénomènes.

La discussion a également abordé la perception erronée de l'IA en tant que solution miracle aux problèmes complexes. Il a été ainsi expliqué que l'IA est un outil d'automatisation et d'optimisation de données, avec des applications telles que la reconnaissance faciale.

L'accent a été mis sur la nécessité d'exploiter l'IA de manière éthique et responsable pour combattre les cybermenaces, tout en prenant en compte les incertitudes liées à son efficacité actuelle. Les intervenants ont souligné la complexité de la fraude dans le domaine de l'IA, la nécessité d'une réglementation européenne adaptée, et la compétence humaine dans le développement d'outils internes.

Toutefois, l'IA peut également être utilisée pour créer ou prévenir des fraudes, comme dans le cas des deepfakes. **L'importance d'une approche scientifique rigoureuse et d'une réglementation adaptée à l'utilisation de l'IA a été soulignée.**

La fraude documentaire, notamment le procédé de morphing, a été abordée comme une préoccupation majeure. Les systèmes de délivrance de documents basés sur l'apport de photos physiques ont été critiqués pour leur vulnérabilité. Les experts ont appelé à une meilleure sécurisation des documents et à une standardisation des actes d'état civil pour contrer efficacement ces fraudes.

Enfin, l'importance de bien comprendre l'IA a été soulignée, ainsi que la nécessité de s'adapter aux innovations futures. La perspective d'une identité numérique liée à des dispositifs personnels a été envisagée, suggérant ainsi une transformation profonde de la gestion des nouveaux usages d'intimité numérique.



Félicien VALLET : IA et protection des données Concilier innovation et protection



IA et protection des données : un nouvel équilibre à trouver

Dans un monde où l'intelligence artificielle (IA) gagne rapidement en importance, la question de la protection des données personnelles se pose avec une acuité nouvelle. C'est sur ce thème crucial que Félicien Vallet, représentant de la CNIL, a axé son intervention récente, soulignant l'urgence d'une prise de conscience collective et d'une régulation adaptée.

La sensibilisation au cœur des préoccupations

Félicien Vallet a insisté sur l'importance de sensibiliser les utilisateurs à la transmission de leurs données personnelles. Dans une ère où la collecte de données est omniprésente, il est indispensable de comprendre quel est le bon destinataire de la transmission. Il a rappelé également la responsabilité des entreprises de se conformer scrupuleusement à la législation en matière de protection des données.

Les principes du RGPD en ligne de mire

Abordant le Règlement Général sur la Protection des Données, Félicien Vallet a énuméré ses principes fondamentaux : la finalité et la minimisation des données, ainsi que la limitation de leur conservation. Le droit d'accès des individus à leurs données personnelles est également un pilier essentiel de ce règlement.

Protection des données et grands événements

Félicien Vallet a également abordé la question de la protection des données dans le contexte de grands événements comme les Jeux Olympiques, une tâche complexifiée par l'implication d'acteurs étrangers et l'utilisation de technologies de surveillance avancées.

Une nouvelle initiative de la CNIL

Dans un effort de mieux comprendre et réguler l'impact de l'IA, la CNIL a annoncé la création d'un service dédié. Cette initiative vise à suivre les évolutions technologiques et à offrir un cadre de guidance aux professionnels, marquant ainsi un pas important vers une régulation adaptée de ces technologies.

Les défis de l'IA face au RGPD

L'intervention a mis en lumière les défis posés par l'IA, notamment en termes de conformité avec le RGPD. Félicien Vallet a évoqué les complexités des systèmes d'IA, les risques de biais et de discrimination, et la difficulté d'auditer ces systèmes pour garantir leur transparence et leur fiabilité.

L'HUMAIN FACE A L'USURPATION D'IDENTITE : COMMENT RESTAURER L'INTEGRITE ?

Si toutes les organisations mettent en place des contraintes réglementaires de contrôle dans la collecte des données identitaires, la plupart négligent néanmoins les effets collatéraux du KYC car elles ne savent pas les identifier. Derrière le KYC il y a un humain, et potentiellement un usurpateur. Lorsque l'humain est victime, il lui est difficile de prouver sa bonne foi, ce qui rend l'escroquerie difficilement réductible.



Cette table ronde a exploré le thème complexe et prégnant de l'usurpation d'identité, ce fléau moderne aux conséquences dévastatrices pour les individus. La discussion a mis en lumière les difficultés et les traumatismes vécus par les victimes, révélant les aspects émotionnels, sociaux, et légaux de ce crime.

Les récits personnels partagés ont dépeint un tableau sombre de l'expérience des victimes : l'arrestation injuste, la perte d'emploi, l'inexistence sociale, et la lutte pour prouver leur innocence. La profondeur de la détresse psychologique, la perte de confiance en soi, et la peur constante d'être pris pour quelqu'un d'autre ont fait la valeur de ces témoignages.

D'un point de vue légal, la discussion a révélé les défis majeurs auxquels les victimes sont confrontées dans le système judiciaire. Le scepticisme des autorités, le manque de coopération internationale, et la relative inefficacité des processus judiciaires ont été soulignés. Les intervenants ont appelé à une réforme législative pour une reconnaissance et une prise en charge plus efficace des victimes, en suggérant une approche globale incluant un soutien juridique, social et psychologique.

En abordant l'aspect technique de l'usurpation d'identité, il a été souligné que les mesures traditionnelles sont souvent insuffisantes pour lutter contre ce phénomène dans l'ère numérique. L'importance de la protection des données personnelles et de l'utilisation de technologies avancées pour contrer les activités malveillantes a particulièrement été mise en avant.



Victimes d'usurpation d'identité : ils témoignent



Nacer AYAD

- **Interdit bancaire** et de crédits pendant **7 ans**
- **12 ans de calvaire**
- **Condamné en 2011 à 11 000 €** à un organisme de crédit
- **Coût de l'avocat : 7 000€**
- **Poursuivi** par des organismes de crédits et banques **qui réclamaient 200 000 € sur 12 crédits à la consommation**
- **1 an de prison avec sursis pour l'usurpateur**



Sylvain BRIANT

- En 2009, copie de sa **carte nationale d'identité utilisée pour des crédit frauduleux et arnaques réalisés**
- **Fiché interdit bancaire, relances incessantes de paiement, passages des forces de l'ordre à mon domicile**
- **Perte d'emploi, dépression nerveuse**
- Le procès pénal contre l'usurpateur a eu lieu en 2019. Il a été condamné à **3 ans de prison dont 2 avec sursis et 3500€ d'amendement sursis et 3500€ d'amende.**



Romain ARGENTIERI

- Victime d'usurpation d'identité depuis **2009**
- Au commencement par de simples **amendes SNCF** puis **vol par escalade, infraction routière, alcoolémie, retrait de permis, hospitalisation**
- **1 dossier de surendettement**
- **2 enfants qui ne portent pas son nom, des saisies à répétition, plus de compte en banque, une obligation de dépendance**



Charlie KOISSI

- Victime d'usurpation d'identité depuis **2008**
- Il reçoit de très **nombreux impayés à régler**
- Il subit une **arrestation pour un mandat d'arrêt européen en plein aéroport**
- Transféré en Allemagne pour **10 ans de prison** à cause de son usurpateur, **il a 24H pour prouver son innocence**
- Découverte de **l'identité du coupable** avec l'aide d'un **criminologue** et d'un **détective privé**
- **Mise en examen** pour un mandat délivré par la **justice polonaise**, avec une **fiche de recherche comprenant la photo de l'usurpateur mais le nom de Charlie KOISSI**

RELATIONS D'AFFAIRES ET IDENTITE : UN DUO À RISQUES ?



La contrainte des démarches à objectif de conquête de clientèle se fait parfois au détriment de la sécurité. Les technologies instantanées négligeant l'aspect sécuritaire génèrent de plus en plus de contentieux. Ceux-ci n'empêchent pas le préjudice et ne constituent qu'une indemnisation par défaut d'anticipation et d'identification du facteur risque.

L'accent a été mis sur les défis inhérents à la gestion de l'identité dans le contexte des affaires, particulièrement dans les secteurs des télécommunications et de la gestion de patrimoine. Les discussions ont révélé la complexité et les risques associés à la vérification des identités dans un monde de plus en plus numérique.

Un des thèmes centraux a porté sur l'importance de la sécurité dans l'ouverture de lignes téléphoniques. La nécessité de procédures de vérification rigoureuses en ligne et en boutique pour prévenir la fraude était également soulignée, tout comme le rôle crucial des opérateurs télécoms dans la sécurité publique.

Les défis rencontrés par les opérateurs télécoms dans la lutte contre la fraude ont été exposés, incluant la gestion des fraudes internes et externes, ainsi que la collaboration avec des groupes de travail spécialisés. Les exemples concrets abordés, ont insisté sur la complexité de ces défis, comme les attaques ciblant les personnes vulnérables pendant les confinements et l'utilisation frauduleuse de documents d'identité.

La discussion a porté également sur le thème central des mesures de sécurité prises par les opérateurs télécoms, notamment la sécurisation des espaces clients en ligne et le contrôle documentaire en boutique, tout en faisant face aux défis de sécurité personnelle des vendeurs.



Dans le secteur de la gestion de patrimoine, les défis de la conformité réglementaire ont été mis en lumière, soulignant la difficulté de se conformer à la législation tout en répondant aux besoins des clients. L'absence d'un référentiel clair et la complexité réglementaire dans ce domaine ont été soulignées, en particulier à travers le risque créé par la fraude documentaire, auquel les procédures KYC classiques ne répondent pas complètement.

La capacité à détecter des documents suspects et à alerter les conseillers sur l'usage frauduleux de documents d'identité a été discutée comme un élément clé dans la prévention de la fraude identitaire. L'importance des bases de données pour vérifier l'authenticité des documents et leur usage, a été mise en lumière en formulant le souhait d'une recherche scientifique et technologique plus audacieuse dans ce domaine.

REPONSES INSTITUTIONNELLES : DES CHIFFRES ET DES MAUX

Face aux difficultés des institutions à quantifier la fraude à l'usurpation d'identité, il est impératif de transformer ce sujet tabou en un débat de société. La fraude exponentielle des dispositifs de solidarités, de protections, ou fiscaux, constitue un préjudice financier pénalisant contribuables et Institutions alors que falsificateurs et fraudeurs mettent en difficulté les services publics et la cohésion nationale. En plus des sanctions pénales, l'utilisation de la technologie devient essentielle dans la lutte contre la fraude.



Cette table ronde a exploré de manière approfondie les enjeux et les défis de la fraude et de l'usurpation d'identité dans notre société numérique. Les discussions ont mis en évidence le rôle crucial des institutions dans l'assistance aux victimes d'usurpation d'identité, notamment par la gestion des incidents de paiement et le traitement du surendettement. Il a été souligné que, malgré l'existence de procédures spécifiques pour les victimes, ces mécanismes rencontrent des limites, en particulier en ce qui concerne la réactivité des banques.

L'évolution des fraudes avec le progrès technologique, notamment le spoofing, a été abordée, mettant en lumière les défis qu'elle pose en termes de prévention et de détection. La complexité de l'annulation et du contrôle des titres d'identité, par rapport à la simplicité d'annulation des cartes bancaires, a été également discutée, ainsi que les bénéfices de la nouvelle carte d'identité numérique.

Un historique de la carte d'identité a été présenté, évoquant ses évolutions et les défis actuels, y compris la transition vers la carte d'identité européenne. Des cas concrets d'usurpation d'identité dans le monde des affaires ont été partagés, mettant en évidence les failles et les répercussions sur les entreprises.

L'importance de la spécialisation judiciaire et la nécessité d'une politique pénale renforcée pour combattre efficacement ces délits a été soulignée. Cette table ronde a clairement illustré la complexité des enjeux liés à l'usurpation d'identité et la fraude, et la nécessité d'une réponse institutionnelle coordonnée et adaptée.



Le mot du politique avec Nicolas DUPONT AIGNAN



Nicolas Dupont-Aignan, député français, a exprimé ses inquiétudes sur la transition rapide vers le numérique, soulignant la vulnérabilité en termes de sécurité et de protection des données. Partageant son expérience d'une escroquerie bancaire subie par sa famille, il a mis en évidence la complexité des fraudes modernes. Il a critiqué la numérisation de la société pour son manque de contrôles adéquats, créant un décalage entre l'essor du numérique et les mesures de sécurité

Il a exprimé des réserves concernant la carte d'identité numérique et européenne, alertant sur les risques de perte de souveraineté et de contrôle excessif, ainsi que la vulnérabilité aux cyberattaques et défaillances techniques. Il a plaidé pour des solutions intégrées incluant prévention, répression, renforcement des moyens judiciaires, et sensibilisation, appelant à une meilleure collaboration entre parlementaires et experts pour développer des solutions efficaces.

DEMARCHE ETHIQUE ET ENGAGEMENT SOCIÉTAL



Lors de la cinquième table ronde, les experts ont abordé la problématique de la cybersécurité et de la fraude identitaire sous l'angle de l'éthique et de l'engagement sociétal.

L'importance de l'humain dans le domaine de la cybersécurité a été ainsi mise en exergue, soulignant que la protection de l'individu doit être au cœur de ses préoccupations. L'unicité de chaque personne, tant physique qu'intellectuelle et morale, protégée par son identité, reste fondamentale dans une société démocratique.

Une approche globale, prenant en compte différents niveaux de protection (individu, organisations, État, Europe, monde libre), était recommandée pour une cybersécurité efficace.

L'évolution rapide des technologies numériques, comme l'intelligence artificielle et les réseaux sociaux, et leur impact sur la dignité et l'intimité des personnes, forment une partie intégrante de la discussion. La nécessité d'une meilleure éducation numérique pour la nouvelle génération était notamment soulignée, en particulier pour prévenir les risques liés à l'usurpation d'identité.

Un autre expert, représentant une fédération d'associations aidant les victimes d'infractions présentait des statistiques alarmantes sur l'augmentation des cas d'escroquerie et d'usurpation d'identité.

Il a évoqué les difficultés rencontrées par les victimes, notamment la preuve de leur innocence et la gestion du stress psychologique. L'idée d'une inversion de la charge de l'effort était suggérée, pour que les professionnels prennent l'initiative d'aider les victimes.



La formation et la sensibilisation aux risques de cybercriminalité étaient jugées cruciales.

Enfin, l'importance de l'aspect humain dans le secteur financier étaient développées par le président d'OPALHE, à travers les initiatives de son groupe pour contribuer à des causes sociétales, notamment un fonds de dotation et le Club.



Le Général Marc Watin-Augouard a mis en avant la nécessité de sensibiliser à la cybersécurité, en se concentrant sur la protection et l'intimité de l'individu. Il a préfacé la bande dessinée, initiative de Marie AZEVEDO, pour souligner ces enjeux et a insisté sur l'importance de l'éducation numérique face aux risques technologiques croissants.

La création d'un fond de dotation européen, destiné aux victimes d'usurpation d'identité a été avancée et aura pour objectif de mettre en place des mesures d'accompagnement par des professionnels, psychologues, enquêteurs. A l'occasion du forum européen, nous avons lancé le label éthique d'entreprises européennes engagées pour la lutte contre la fraude, qui s'inscrit dans la démarche Engagé RSE de Afnor certification entreprise par RESOCOM Groupe.



SYNTHESE ET CONCLUSION DE LA JOURNEE

Béatrice BRUGÈRE

Béatrice Brugère, Secrétaire Générale d'Unite-Magistrats SNM-FO, a éclairé plusieurs points cruciaux concernant la justice et la cybercriminalité. Elle a débuté par une présentation de son rôle de magistrate et de dirigeante syndicale, insistant sur l'importance de la coopération et du partage d'informations pour améliorer l'efficacité de la chaîne pénale.

Béatrice Brugère a reconnu que de nombreux magistrats, sauf ceux spécialisés, manquent de connaissances approfondies des enjeux spécifiques de la cybercriminalité. Elle a critiqué l'absence d'une méthodologie claire dans l'approche française en matière de stratégie face à ces défis. Elle a souligné **le rôle de l'État et la nécessité d'une responsabilité collective, impliquant entreprises et associations, pour affronter les défis actuels, tout en mettant l'accent sur l'éthique et les valeurs comme la vérité et la liberté.**

Elle a discuté de la manière dont différentes approches nationales envers les données et l'intelligence artificielle reflètent les idéologies sous-jacentes. Elle a insisté sur l'importance de prendre des risques dans la prise de décision et de réintroduire l'humain dans ce processus. Identifiant l'usurpation d'identité comme un crime grave lié à la criminalité organisée, elle a appelé à une approche globale et transversale pour y faire face.



Pour finir, Béatrice Brugère a encouragé une vision globale et la mobilisation de ressources pour lutter contre la criminalité croissante, en insistant sur la nécessité d'une meilleure organisation, d'une mise à niveau technologique et d'une collaboration étroite entre tous les acteurs du système judiciaire.



Marie AZEVEDO, Présidente de l'association du RESOCLUB EFP

Clôture du 8e forum européen de lutte contre la fraude

Dans son discours de clôture, Marie Azevedo a souligné plusieurs points essentiels. Elle a commencé par mettre en lumière la lenteur des réactions face à la cybercriminalité, en comparant la fraude à la calomnie où quelque chose persiste malgré les efforts pour l'éliminer. Marie Azevedo a insisté sur la nécessité d'un accompagnement approfondi des victimes, bien au-delà des simples offres d'indemnisation, soulignant l'importance de l'écoute et de l'empathie pour aider à la reconstruction.

Elle a également parlé de la création d'une bande dessinée durant le confinement, une initiative visant à sensibiliser au vécu des victimes de fraude, avec l'aide d'un artiste graphique. Marie Azevedo a remercié les partenaires comme le groupe Opalhe et France Victimes pour leur soutien dans la construction d'un réseau de soutien et de sensibilisation aux problèmes de fraude et d'usurpation d'identité.

L'annonce de la création d'un label pour reconnaître et valoriser les initiatives en faveur des victimes a été un autre point clé de son discours. Elle a souligné l'importance de l'approche pédagogique et de la sensibilisation, évoquant la mise en place d'ateliers et de rencontres pour débattre des enjeux liés à la fraude et à l'usurpation d'identité.

Pour conclure, elle a exprimé sa détermination à agir et sa conviction que l'espoir réside dans une action résolue et une solidarité collective, afin de soutenir les victimes et de leur permettre de surmonter leurs épreuves.



L'art contemporain comme symbolique de l'action du groupe RESOCOM



L'artiste sculpteur Ghass était également présent à l'événement avec son oeuvre "la Marianne".

Ghass partageait son parcours personnel avec les participants au forum, depuis l'Iran jusqu'à la France, où il évoquait notamment son engagement dans la défense des droits des femmes. Il décrivait son travail sur la Marianne comme une oeuvre symbolisant une femme libérée, une initiative inspirée par la situation des femmes dans son pays natal et dans le monde.

Marie Azevedo reliait ainsi la symbolique de la Marianne "brisant ses chaînes" à la lutte contre l'usurpation d'identité, en soulignant la nécessité de rompre avec l'idée que l'usurpation d'identité est une fatalité de notre époque, alors qu'une réponse globale et résolue reste possible pour lutter contre son expansion.

MERCI À VOUS D'AVOIR RENDU CELA POSSIBLE



DIRECTION GENERALE DE LA POLICE NATIONALE



EUROSISTÈME



Vous êtes victime d'usurpation d'identité ?

Vous pouvez être accompagné

SOSVICTIMES@IDVERIF.COM

• Soutien Juridique



• Soutien Psychologique



• Soutien par des experts



N'hésitez plus, faites entendre votre parole

