IDEMIA
augmented identity

REPONSE D'IDEMIA A LA CONSULTATION PUBLIQUE DE LA CNIL

relative aux conditions de déploiement des caméras dites "intelligentes" ou "augmentées" dans les espaces publics

Date
10/03/2022

Document Ref.
EU/BG/ 2022-41399

Version du Document
01-00

TABLE DES MATIERES

Introduction

Leader mondial en matière de gestion des identités d'accès, et de biométrie, c'est en tant que fournisseur de systèmes d'intelligence artificielle parmi lesquels des logiciels de vidéo augmentée, qu'IDEMIA souhaite répondre à la consultation de la CNIL. IDEMIA place les besoins du client et la protection du citoyen au cœur de toutes ses actions. Nous combinons les préoccupations premières que sont la sécurité, le facteur humain, la facilité d'usage et la continuité des services dans une proposition de valeur unique, entièrement intégrée.

De nouvelles tendances viennent transformer notre monde : la nécessité de mettre en place des solutions sécurisées dans les secteurs privé comme public, la migration des services vers un monde de plus en plus numérique et la demande croissante des individus pour des expériences utilisateurs toujours plus sûres et plus intuitives. Parallèlement, dans le « monde d'après » COVID-19 les citoyens aspirent à des interactions plus fluides tout en se sentant protégés. Face à ces mutations, IDEMIA envisage la sécurité dans toutes ses dimensions, au-delà des développements techniques, en prenant en compte la manière dont la technologie est utilisée.

Devant le constat du déploiement de la vidéo augmentée, un débat public avec l'ensemble des parties prenantes était nécessaire. IDEMIA accueille très favorablement cette consultation publique, et apprécie les définitions claires et précises des concepts que la CNIL rappelle dans son projet de doctrine. IDEMIA approuve également la nécessité d'une évolution du cadre normatif qui entoure la vidéo augmentée.

Néanmoins, IDEMIA regrette que la CNIL, après avoir appelé à un débat autour de la reconnaissance faciale dans sa note du 15 novembre 2019, écarte celle-ci du périmètre de la présente consultation.

La reconnaissance faciale représente pourtant l'une des fonctionnalités d'avenir de la vidéo augmentée, même si, en l'état actuel du droit, la majorité des analyses est réalisée sans avoir recours à des traitements de données biométriques. Or, si un consensus existe, au niveau européen, pour interdire l'utilisation de systèmes ayant pour objectif la surveillance de masse de la population, il demeure que l'usage de systèmes de vidéo augmentée aux fins d'application de la loi doit faire l'objet d'un encadrement légal strict, en particulier dans ses implémentations en temps réel. Dans ces circonstances, il aurait été bienvenu de permettre aux différentes parties prenantes d'exposer leurs réflexions, pour enrichir le débat autour de cette technologie et de ses usages.

La vidéo augmentée, et la multiplicité des cas d'usage qu'elle offre interroge l'éthique sous des prismes très divers : la maîtrise et la responsabilité humaine, la fiabilité technique et la sécurité, la protection de la vie privée, la transparence et l'explicabilité, le risques de biais contraires à l'équité ou à la non-discrimination, le bien-être collectif ou encore l'auditabilité. Parfois, ces principes entrent en contradiction les uns avec les autres : la transparence algorithmique peut affaiblir la sécurité et faciliter les attaques, le respect de l'équité implique de collecter plus de données que ne le commanderait le principe de minimisation, la performance peut être négativement corrélée à la minimisation des données, etc. Des compromis sont alors nécessaires, qui doivent être documentés et justifiés, en France et en Europe plus que partout ailleurs.

IDEMIA saisit donc l'opportunité offerte par la CNIL pour présenter ses défis (Section 1), ses réflexions (Section 2) et ses propositions (Section 3), des points de vue technique, éthique et juridique, en qualité de fournisseur de logiciel de vidéo augmentée. Compte tenu de ses relations historiques avec les autorités publiques ayant pour mission d'assurer la sécurisation des lieux et des personnes, c'est essentiellement autour de ces cas d'usage que les réflexions d'IDEMIA se concentrent.

Pour clarté du propos, l'emploi par IDEMIA dans ce document du terme « Vidéo augmentée » recouvre toute surcouche logicielle permettant le traitement automatisé de flux de vidéos, quel qu'en soit le support physique.

Section 1. Les défis de la vidéo augmentée pour les industriels français tels qu'IDEMIA

1.1. Les défis sociétaux :

Le premier défi auquel se heurte IDEMIA est celui du manque d'information de l'opinion publique sur le sujet.

Si l'on prend l'exemple de la vidéoprotection, telle que définie dans l'appel à la présente consultation, elle paraissait à l'origine attentatoire à la vie privée. Mais la loi de 1995 a conditionné son déploiement à de très nombreuses garanties, sous le contrôle de la CNIL. La loi institue un régime d'autorisation administrative accordée pour une durée de cinq ans sur la base d'un cahier des charges juridique et technique protecteur pour les libertés individuelles. L'opinion publique a progressivement évolué vers un consensus face aux apports de la vidéoprotection pour la sécurité collective. Par exemple, l'utilisation de la vidéoprotection dans l'identification des auteurs d'attentats terroristes a contribué à modifier la perception de ces dispositifs. Le contentieux relatif à la vidéoprotection est du reste très faible. La perception sociale de la vidéoprotection peut aussi être modifiée par une évolution du rapport à l'image à l'ère des réseaux sociaux.

Un effort de sensibilisation de l'opinion publique aux bénéfices apportés par la vidéo augmentée ajoutée à la vidéoprotection doit être donc entrepris.

L'autre défi auquel le déploiement de la vidéo augmentée est confronté est celui de la définition de ce qui est acceptable d'en faire. En effet, il existe une multiplicité de cas d'usages qui ont été soumis à la CNIL pour demande de conseil. S'il n'appartient pas à IDEMIA en tant que fournisseur de logiciel d'en décider, nous souhaitons toutefois insister sur les bénéfices réels de la technologie pour l'accomplissement de leurs missions de service public par nos clients (cf infra Section 2).

1.2. Les défis économiques et techniques :

Les exigences qui pèsent sur les fournisseurs français de cette technologie sont importantes et engendrent des coûts additionnels. Elles impactent de nombreux aspects du développement et du cycle de vie de nos produits, comme la sécurité des données ou la documentation. Les analyses techniques et juridiques nécessaires afin de se conformer aux règlementations applicables sont également coûteuses. Ce surcoût indispensable doit être bénéfique, à la fois pour les utilisateurs et pour les concepteurs de ces produits.

1.3. Les défis juridiques :

En l'absence de législation spécifique à la vidéo augmentée, l'application stricte du Règlement général pour la protection des données (ci-après le « **RGPD** ») et de la loi Informatique et Libertés entraine une situation dans laquelle les expérimentations sont difficiles à mettre en œuvre. Or, sans expérimentations, la démonstration des bénéfices attendus est impossible. Il est également impossible de démontrer que les systèmes répondent totalement aux impératifs de préservation des libertés fondamentales.

L'application stricte du RGPD engendre également des défis en termes de performance : les concepteurs européens et français sont soumis à des contraintes, certes légitimes, mais fortes

s'agissant de la collecte des données d'apprentissage, de leur durée de conservation, etc. qui peuvent freiner les capacités d'innovation voire la performance des algorithmes, notamment lorsqu'ils sont basés sur le *machine learning*. Or, c'est certainement l'une des explications à la performance technologique de certains acteurs étrangers (chinois, russes, israéliens), dont les activités d'innovation et de développement ne sont pas encadrées aussi strictement.

Le respect de ces contraintes doit donc pouvoir être valorisé par une forme d'étiquette ou de label, lors d'une mise sur le marché, et se transformer en avantage compétitif, afin de rééquilibrer l'égalité des chances dans ce marché mondial. C'est l'une des propositions d'IDEMIA (cf infra Section 3).

Enfin, IDEMIA reconnait que réguler une technologie dont les cas d'usage sont hétérogènes, comme c'est le cas pour la vidéo augmentée, suscite une difficulté fondamentale, qui réside dans l'approche à retenir. Cette approche peut être sectorielle (en fonction du secteur industriel concerné) ou basée sur les risques (en fonction des risques d'atteinte aux droits et libertés des personnes concernées par la technologie). IDEMIA, en tant que fournisseur d'une telle technologie, souhaite bénéficier d'un cadre normatif spécifique, adapté à ses propres enjeux, et qui soit clair et juste pour guider l'innovation.

Section 2. Nos réflexions sur les bénéfices de la vidéo augmentée dans l'espace public

2.1. Des bénéfices avérés dans l'usage aux fins d'enquête

L'intérêt de la vidéoprotection est indiscutable pour les enquêteurs et représente une aide certaine aux personnels de voie publique. L'ajout de capacités d'analyse automatisées aux systèmes de vidéoprotection existants permet d'accélérer considérablement les temps d'analyse après un événement, et de fournir des pistes à exploiter plus rapidement aux enquêteurs. L'efficacité de leurs missions est renforcée.

2.2. L'usage en temps réel

L'efficacité des caméras de vidéoprotection en temps réel est aujourd'hui plus discutée et doit être renforcée, justement à l'aide de dispositifs d'analyse automatisée : la multiplication des caméras et des sites publics protégés entraine un accroissement du nombre d'écrans surveillés par les opérateurs. Le recours aux caméras tournantes ajoute des difficultés d'interprétation. En conséquence, certaines infractions commises ne sont pas repérées par les opérateurs : l'exemple de l'attentat de l'église de Nice en octobre 2020 est parlant. Alors que le site était dans le champ d'une caméra de vidéoprotection dédiée, c'est le recours à une alarme coup de poing actionnée par un témoin qui a permis d'alerter les services de police de la survenance de l'attaque et pas l'opérateur.

En partant de ce constat, les acteurs de la sécurité demandent à la technologie de leur venir en aide via l'intelligence artificielle : le déclenchement d'une alarme grâce au système d'analyse automatisé peut permettre une intervention plus rapide.

Ceci permet également une meilleure allocation du personnel. La vidéo augmentée permettrait de réduire le nombre d'agents chargés de l'exploitation des flux des caméras de vidéoprotection, au bénéfice d'agents sur le terrain, plus vite (stratégie des feux naissants) et donc plus directement au service des citoyens. Les informations générées par les systèmes de vidéo augmentée permettent d'ailleurs à des agents de terrain de largement améliorer leur compréhension de la situation avant d'intervenir, sans se reposer exclusivement sur la description de la situation et des instructions d'un poste central.

Dans la sphère de la vidéoprotection, le recours à l'intelligence artificielle à des fins d'analyses représente une avancée par rapport au respect des libertés, comme nous le soutenons ci-après.

2.3. Les biais humains

Aujourd'hui, c'est le cerveau exercé d'agents surveillant les murs d'images qui leur permet de repérer les comportements anormaux et de réagir. Or, bien que les informations provenant des caméras soient spécifiques et mesurables, les agents qui les regardent, en tant qu'êtres humains, sont sujets à des biais cognitifs et émotionnels. Nous sommes tous sujets à des biais attentionnels qui naturellement et inconsciemment filtrent notre perception, en créant soit des angles morts, soit au contraire des points focaux.

Aujourd'hui ces biais sont difficiles à contrôler et à mesurer et ils évoluent au cours du temps, ce qui peut donc fortement biaiser l'écosystème de vidéoprotection. Dans le même ordre d'idées, il a été démontré que les récits des témoins oculaires sont soumis à de multiples biais qui minent leur valeur probante.

Les flux provenant des caméras de vidéoprotection étant en permanence projetés sur les murs d'images et regardés par des opérateurs, aucune information ne peut être qualifiée de dormante. Ceci implique qu'il y a un risque avéré que des informations puissent être collectées par ces opérateurs de manière inconsciente ou non. Cela pourrait mener à des dérives.

2.4. Les biais algorithmiques

S'agissant des biais, le recours à l'intelligence artificielle par rapport à l'humain apporte au moins deux avantages certains :

- Le premier est qu'avec l'intelligence artificielle, nous avons une chance unique d'identifier et de quantifier les biais liés à ces systèmes.
- Le second est que, dans le cas d'une identification biométrique, les seules personnes susceptibles de déclencher une action du système sont celles dont le profil biométrique aura été préalablement inséré dans une base de personnes d'intérêt, selon un cahier des charges juridique et technique protecteur pour les libertés individuelles. S'appuyer sur la mémoire des opérateurs humains est une entreprise beaucoup plus risquée et moins contrôlable. Par ailleurs, les alarmes générées par le système doivent faire l'objet d'un examen supplémentaire par un opérateur humain, réduisant en pratique des erreurs possibles à un nombre extrêmement faible[1].

Actuellement aucun industriel ne peut se prévaloir de fournir une solution dont les algorithmes ne commettent aucune erreur. La grande différence ici repose sur le fait que ces biais peuvent être scientifiquement mesurés alors que les biais humains le sont très difficilement. De plus les biais algorithmiques ne varieront pas au cours du temps.

Face à ce constat, nous pensons qu'il serait souhaitable de définir et de mettre en place une norme internationale sur les biais des solutions d'analyse vidéo. Cela permettrait de s'assurer de manière certaine de la limitation au maximum de tout biais dans l'écosystème de vidéoprotection.

2.5. Des bénéfices attendus

Ainsi à terme nous pourrions imaginer des salles vidéo aux écrans éteints, et donc une liberté d'aller et de venir retrouvée.

Seules les situations à risque, les infractions telles qu'une agression, ou la présence d'un véhicule dans une zone piétonne, ou les situations classées nativement comme dignes d'intérêt, déclencheraient la visualisation des images par les opérateurs afin de leur permettre de réagir. En cas d'identification biométrique par exemple, l'identité des individus impliqués pourrait d'ailleurs n'être accessible à

[1] Alice O'Toole et Carlos D. Castillo (*Face Recognition by Humans and Machines: Three Fundamental Advances from Deep Learning*

l'opérateur qu'une fois le caractère dangereux de la situation validé par lui, et ce, de manière également auditable au travers des logs du système.

Les observations indues, qu'elles soient volontaires ou fruits du hasard, disparaissent dès lors totalement. Chaque caméra aura alors l'efficacité d'une patrouille expérimentée, sans avoir les dérives potentielles énoncées plus haut.

Section 3. Nos propositions pour l'avenir de la vidéo augmentée

3.1. Propositions juridiques

IDEMIA milite pour une règlementation spécifique à la vidéo augmentée, qui retiendrait une approche par les risques, avec une définition et une catégorisation claire de ces risques, ainsi que la promotion d'une méthode harmonisée pour évaluer ces risques, et leur mode de remédiation. IDEMIA souhaite également voir dissocier juridiquement la phase d'apprentissage, par rapport au droit positif actuel des traitements de données.

Nous recommandons de construire un cadre assoupli sur certains critères comme la durée de conservation ou le fait que seules les données caractérisant de manière avérée tel ou tel événement (par exemple une menace) soient utilisées. D'autres garanties peuvent parfaitement être apportées en contrepartie : exclusion de tout usage opérationnel pour les données d'entraînement, conservation par un tiers de confiance indépendant, pseudonymisation dans toute la mesure compatible avec la finalité d'apprentissage visée etc.

3.2. Propositions techniques

3.2.1. Une traçabilité totale

L'avantage de la mise en place de systèmes de vidéo augmentée réside notamment dans l'amélioration de la traçabilité des traitements menés et augmente donc la transparence des dispositifs.

Un système automatisé permettrait, si les mécanismes sont mis en place, de tracer automatiquement et de manière sécurisée toutes les actions du système et de ses utilisateurs. Ces logs seraient stockés de manière sécurisée et pourraient être utilisés :

- En cas d'audit par les autorités compétentes afin de s'assurer qu'aucune dérive n'a eu lieu ;
- En cas de dérive avérée afin d'investiguer dans le détail ce qui s'est passé.

Définir clairement quels logs devrait obligatoirement effectuer un système de vidéo augmentée nous semble également primordial.

3.2.2. Assurer la sécurité des données

Il est essentiel que toutes les données stockées ou générées par le système d'analyse de vidéo augmentée (vignettes, images extraites des vidéos lors d'une détection ou alerte, métadonnées générées, ou logs) soient chiffrées. Cela permettait d'éviter un accès illégitime à ces données, potentiellement sensibles. Dans le même ordre d'idées réaliser des tests de sécurité poussés est indispensable afin de s'assurer de l'absence de portes dérobées dans le système.

De même, ce type de système devrait être doté d'un contrôle d'accès à base de rôles. On s'assurerait ainsi que les opérateurs n'ont accès qu'aux données qu'ils ont besoin de connaître. Ce mécanisme est également indispensable pour assurer une bonne traçabilité du système.

3.3. Propositions éthiques

Le rapport « Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne (2018) » esquisse plusieurs pistes qu'IDEMIA fait siennes. En amont, il s'agit d'intégrer les enjeux éthiques dès la formation des ingénieurs et la conception des outils d'intelligence artificielle. L'appropriation et la compréhension de ces technologies doit aussi être favorisée en en favorisant l'« explicabilité », en conduisant un débat public informé, voire en développant l'évaluation citoyenne plus en aval. D'une façon plus générale, des systèmes de contrôle et d'évaluation doivent être mis en place par le développement de l'audit (le rapport propose la création d'un corps d'experts publics assermentés). Au niveau stratégique, ces technologies pourraient faire l'objet d'une supervision par un comité d'éthique ad hoc, sur le modèle du Comité national d'éthique.

A ces propositions, IDEMIA souhaite ajouter les suivantes :

3.3.1. Une liste des fonctions de détection algorithmique autorisées :

Le nouveau cadre normatif devrait définir une liste stricte et explicite des fonctions de détections algorithmiques autorisées. Cette liste devrait être dressée en amont et indépendamment de leur hypothétique installation. Elle se devrait d'être évolutive afin de prendre en compte les avancées technologiques sur le marché ainsi que le retour d'expérience sur le terrain.

3.3.2. Un déontologue aux côtés des utilisateurs

IDEMIA propose la mise en place d'un nouveau rôle, au sein des entités utilisatrices de ces technologies. Il pourrait s'agir d'un déontologue qui serait un tiers indépendant chargé d'assister les opérateurs, et qui pourrait également assumer des fonctions de formation continue, voire d'audit ou de contrôle interne au sein de ces entités. Ce déontologue veillerait au respect des grands principes posés par le RGPD, ainsi que plus généralement, au respect des libertés individuelles.

3.3.3. Des outils d'aide à la décision

Enfin, le maintien d'une main humaine dans la prise de décision et le contrôle des technologies est primordial. Les algorithmes d'intelligence artificielle sont en premier lieu des outils d'aide à la décision. Ils peuvent intervenir à des degrés variables dans la prise de décision, selon la complexité des enjeux, mais, s'ils bénéficient d'une forme d'autonomie, ils doivent toujours être susceptibles d'une reprise en main ou d'un contrôle direct ou *a posteriori* de la part d'opérateurs.

3.4. Label CNIL/ANSSI

IDEMIA serait favorable à la création d'un label de certification du ressort exclusif d'une entité indépendante telle que la CNIL ou l'ANSSI. Une telle certification permettrait de s'assurer que tout est mis en œuvre afin de respecter les libertés individuelles et la sécurité des données. Cette certification reprendrait l'ensemble des points évoqués dans ce chapitre de propositions.

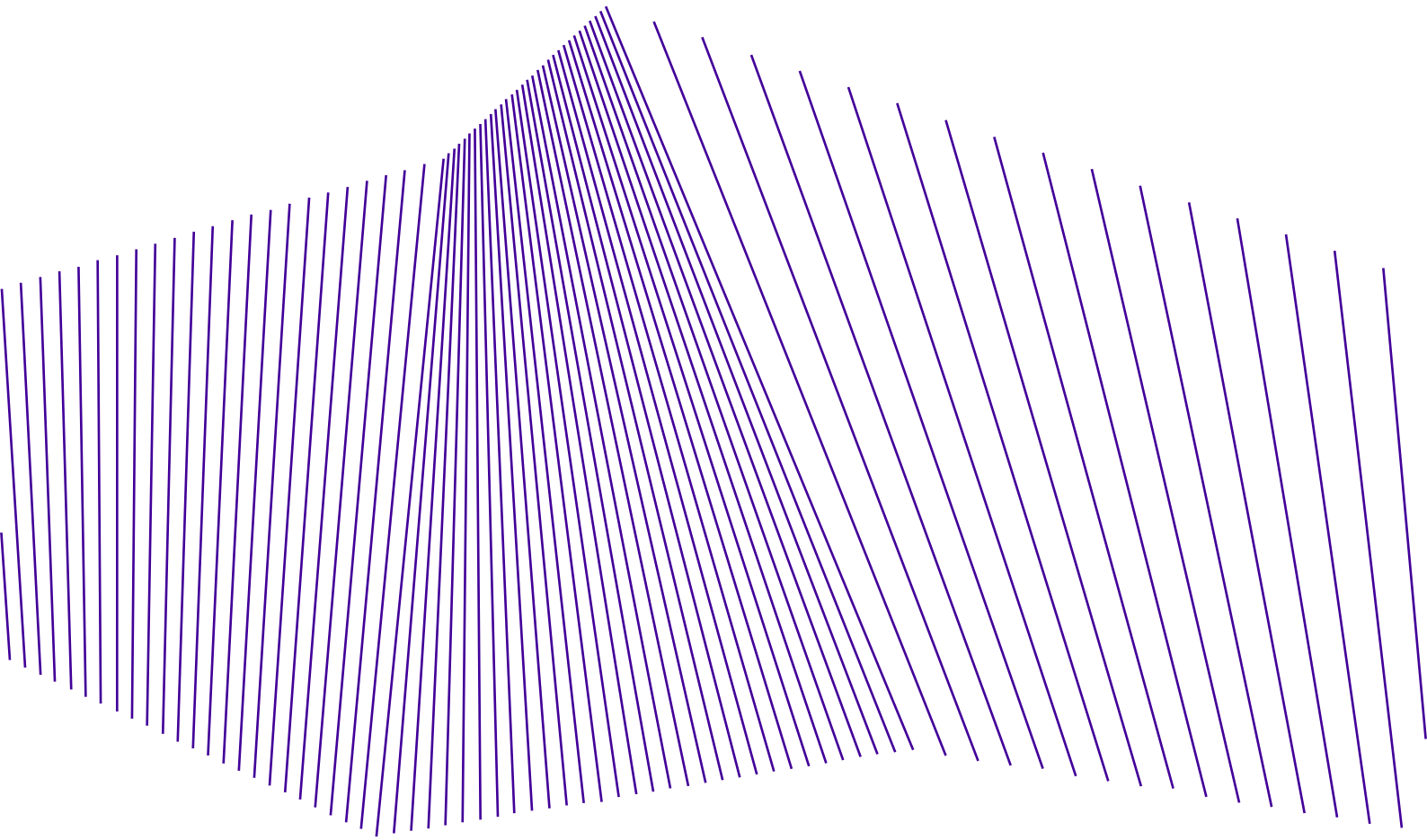
L'obtention de ce label serait obligatoire à la commercialisation de toute solution de vidéo augmentée sur le territoire français.

Conclusion

IDEMIA se tient à la disposition de la CNIL et des pouvoirs publics pour poursuivre le débat et présenter plus en détail ses propositions. IDEMIA souhaiterait également pouvoir prendre connaissance des analyses des parties prenantes au débat lancé dans le cadre de cette consultation, afin de poursuivre ses réflexions.

La compréhension de l'acceptabilité par le public de la vidéo augmentée est une question qui relève du pouvoir législatif et des élus locaux qui doivent également se faire entendre dans le cadre de cette consultation.

IDEMIA souhaite que le cadre normatif à venir reflète les enjeux révélés à travers une consultation réfléchie et complète. Ceci est en faveur des citoyens qui doivent être en mesure de faire confiance à l'ensemble de l'écosystème de la vidéo augmentée, et être sûrs que ce qui est technologiquement possible soit à la fois légalement permis et socialement acceptable.



IDEMIA
augmented identity

Join us on

www.idemia.com