Tel 01 48 05 47 88
Mail : contact@syndicat-magistrature.org
Site : www.syndicat-magistrature.fr
Twitter : @SMagistrature

Paris, le 17 février 2023

« UTILISATION D'IMAGES DE SÉCURITÉ DANS LE DOMAINE PUBLIC DANS UNE FINALITÉ DE LUTTE CONTRE L'INSÉCURITÉ »

Réponses du Syndicat de la magistrature[1] aux questions de la mission d'information de la commission des lois de l'Assemblée nationale

Les réponses qui suivent sont issues de la consultation de nombreux magistrats, ce qui nous a notamment permis de constater, en dehors de quelques spécialistes, une relative indifférence voire méconnaissance par nos collègues des enjeux attachés à l'utilisation de techniques biométriques – voire même du cadre légal dont ils sont garants – inversement proportionnelle au rôle attendu de l'autorité judiciaire en cette matière. De ce point de vue, votre mission d'information est particulièrement bienvenue au regard de la place de plus en plus importante accordée à l'image, tant dans le procès pénal que dans la perception de son utilité en matière de sécurité.

Nous faisons le constat d'une tendance générale aveuglément orientée vers l'extension de l'utilisation des technologies de surveillance, la vidéo-surveillance – si possible automatisée – étant décrite comme l'alpha et l'omega de la sécurité, voire même de la preuve pénale. Pourtant, l'attente des citoyens semble finalement beaucoup plus nuancée que celle des acteurs économiques du secteur, convoitant un marché que l'on sait extrêmement lucratif, mondial et en pleine expansion : nous avons ainsi lu avec intérêt le rapport du Défenseur des droits d'octobre 2022, révélant notamment que *« Si les Français font confiance aux institutions régaliennes pour avoir une utilisation raisonnée des technologies biométriques,* ***il n'existe pas de soutien inconditionnel à un usage généralisé de ces technologies dans l'espace public****. 63 % s'opposent à ce que l'on puisse les reconnaître et les identifier sans qu'ils ne le sachent »*[2]. Malgré cette opposition large de nos concitoyens à un développement illimité du recours à l'image en matière de sécurité et de justice, le projet de loi JO 2024 – et plus particulièrement son article 7 prévoyant une expérimentation de la video-surveillance algorithmique – nous conduit à constater l'absence de volonté politique de freiner ce mouvement devenu quasi-inexorable au regard des dépenses déjà engagées, d'ailleurs renforcées par l'adoption récente de la loi de programmation pour le ministère de l'Intérieur[3].

---

1 Organisation représentative de magistrats, le Syndicat de la magistrature est également membre fondateur et actif de l'Observatoire des libertés et du numérique (OLN), regroupant de multiples organisations depuis 2014, dont l'objet est notamment de contribuer à l'amélioration des textes fondateurs en matière de protection des données personnelles et de veiller à la mise en œuvre d'une politique du numérique respectueuse des droits, ce qui passe nécessairement par dispositifs de contrôle effectifs des fichiers et des technologies de surveillance actuelles

2 https://www.defenseurdesdroits.fr/fr/etudes-et-recherches/2022/10/enquete-perception-du-developpement-des-technologies-biometriques-en

3 Plusieurs mentions du rapport annexé font ainsi état de l'augmentation considérable des crédits affectés à la vidéo-protection

Or, d'après les consultations que nous avons menées et, plus largement, de nos travaux avec les autres membres de l'Observatoire des libertés et du numérique, si une expérimentation paraît souhaitable, ce n'est pas celle de nouvelles technologies de surveillance généralisée par intelligence artificielle, mais plutôt l'expérimentation d'un droit permettant d'encadrer de façon stricte et effective par l'autorité judiciaire le recours à ces technologies et à leurs usages, en offrant toutes les garanties nécessaires pour éviter le moindre détournement.

En résumé, notre conviction profonde est que l'urgence n'est pas de faire évoluer le droit pour permettre l'utilisation plus large de ces technologies, mais au contraire afin de mieux l'encadrer.

1. **Que pensez-vous du recours aux techniques de reconnaissance faciale par les forces de sécurité afin de comparer une image aux photographies contenues dans les fiches des personnes mises en cause au sein du TAJ ? Quel est le contrôle opéré par l'autorité judiciaire en la matière ?**

Les techniques de reconnaissance faciale utilisées pour exploiter le fichier « TAJ » relèvent de la catégorie juridique de « traitement (automatisé) de données biométriques » au sens de la loi informatique et libertés du 6 janvier 1978. Il s'agit, par conséquent, d'une dérogation à l'interdiction de principe posée par ce texte, justifiant que le contrôle du respect des conditions de cette dérogation soit strict.

À ce titre, nous regrettons l'interprétation particulièrement large qu'a récemment pu donner le Conseil d'État[4] à la condition de « nécessité absolue » du recours à ces traitements automatisés, pouvant se résumer à l'argument suivant lequel il y a tellement de photos dans le TAJ qu'il existe une nécessité absolue de recourir à un algorithme de traitement automatisé des données biométriques pour pouvoir l'exploiter utilement. Le Conseil d'État a, en revanche, été moins péremptoire sur la nécessité absolue d'utiliser le TAJ et les algorithmes de reconnaissance faciale pour la recherche des auteurs d'infractions et la prévention des atteintes à l'ordre public : « *une telle identification à partir du visage d'une personne et le rapprochement avec les données enregistrées dans le TAJ* ***peuvent*** *s'avérer absolument nécessaires à la recherche des auteurs d'infractions et à la prévention des atteintes à l'ordre public* ».

Les remontées de terrain que nous avons obtenues sur cette question sont d'ailleurs assez révélatrices du regard beaucoup plus nuancé que portent les magistrats (plus particulièrement les magistrats du parquet, les juges d'instruction, ou les juges correctionnels) sur la force probante et l'utilité des résultats ainsi obtenus et donc, *a fortiori*, sur cette idée de « nécessité absolue » d'y recourir (voir *infra*, question n°3).

S'agissant du contrôle judiciaire de l'utilisation des techniques de reconnaissance faciale par les policiers, gendarmes et douaniers, elle repose tout d'abord sur l'existence d'un fichier, dont la gestion est actuellement censée être contrôlée par l'autorité judiciaire. Cependant, ce contrôle se révèle, en pratique, largement insuffisant.

La loi prévoit ainsi plusieurs types de contrôle par l'ensemble des procureurs de la République ainsi que par un magistrat à compétence nationale (art. 230-8 et 230-9 du code de procédure pénale) : contrôle de la *« mise en œuvre du traitement »* ou de sa *« mise à jour »* par le magistrat national référent (art. 230-9 et R.40-32 du code de procédure pénale), traitement *« opéré sous le contrôle »* du procureur de la République territorialement compétent, qui aura à connaître des demandes de rectification ou de suppression. Sur ce point, les pratiques sont particulièrement inégales sur le territoire, certains parquets ayant un magistrat référent, d'autres non, mais la pratique habituelle semblant plutôt être celle d'un suivi assez superficiel des opérations concernant l'inscription ou la

[4] https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2022-04-26/442364

suppression des fiches TAJ, sans comparaison possible avec la façon dont sont suivies les requêtes relatives au casier judiciaire, alors même qu'une inscription au TAJ a finalement des conséquences pratiques de même gravité pour les intéressés. Il est donc permis d'affirmer que le TAJ est bien loin d'être un fichier fiable pour ce qui concerne la situation pénale des personnes fichées comme potentiels auteurs d'infractions.

S'agissant du magistrat national référent prévu par les articles 230-9 et R. 40-32 du code de procédure pénale, il est censé pouvoir être directement saisi de requêtes de justiciables, mais il est concrètement impossible, en l'état des portails numériques du ministère de la Justice, d'être informé sur les conditions de sa saisine (pas de formulaire CERFA, pas de notice, pas d'adresse). De même, le rapport annuel, dont ce magistrat a la charge, est également parfaitement introuvable, y compris sur l'intranet du ministère de la justice, ce qui ne permet pas de connaître concrètement l'étendue du contrôle opéré. Il pourrait, à ce titre, être utile d'en prévoir une diffusion plus large.

Enfin, le contrôle des cas précis d'utilisation de ce traitement *automatisé* des données personnelles (c'est-à-dire, notamment, de l'algorithme de reconnaissance faciale, permettant, en injectant une image dans le TAJ, de trouver la ou les fiches qui lui pourraient lui correspondre) est également prévu par le code de procédure pénale, qui reste néanmoins muet sur les conditions concrètes de ce contrôle. Mise en place depuis peu de temps, cette fonction du TAJ est désormais utilisée de façon massive en police judiciaire, bien au-delà du cadre légal de la recherche d'auteurs d'infractions, par la longue liste des agents habilités sur le fichier TAJ (R. 40-28 et s. CPP).

C'est ainsi que ce mécanisme peut, en pratique, être utilisé dans le cadre de simples contrôles d'identité, sans aucun moyen pour l'autorité judiciaire de l'empêcher. Les dispositions du dernier alinéa de l'article 55-1 du code de procédure pénale issues de la loi du 24 janvier 2022, prévoient pourtant que l'utilisation d'une photographie prise sans le consentement de la personne concernée doit répondre à des conditions très strictes : il doit s'agir d'une photographie constituant l'unique moyen d'identifier une personne entendue dans le cadre d'une enquête de flagrance *« pour un crime ou un délit puni d'au moins trois ans d'emprisonnement et qui refuse de justifier de son identité ou qui fournit des éléments d'identité manifestement inexacts »*, cette opération ne pouvant par ailleurs se faire que *« sur autorisation écrite du procureur de la République saisi d'une demande motivée »* par l'officier de police judiciaire.

Les retours de terrain que nous avons obtenus démontrent qu'il existe au contraire une pratique très répandue d'utilisation de la nouvelle fonctionnalité du TAJ de recherche par images en injectant des photographies issues de multiples sources (réseaux sociaux, vidéo-surveillance, etc.) et, en toute hypothèse, sans consentement de l'intéressé. En effet, grâce à l'importance du nombre de photos alimentant le TAJ, ce mécanisme est décrit comme étant aujourd'hui très performant – après quelques difficultés rencontrées au moment de l'ajout de cette nouvelle fonctionnalité – pour trouver des liens entre une photographie (même de mauvaise qualité) avec une fiche du TAJ.

L'on peut donc légitimement craindre que le détournement de cette technologie devienne la norme sans que rien ne puisse l'entraver. Or, si les consultations du TAJ et les utilisations du dispositif par les agents habilités font l'objet d'un « traçage » consultable par les autorités de gestion du fichier, le contrôle de ces utilisations est humainement impossible au regard de leur nombre. Il doit s'en déduire que l'utilisation de cette technologie est en pratique illimitée pour les forces de sécurité.

Dans ces conditions, nous ne partageons pas, loin s'en faut, la conclusion du Conseil d'État dans sa décision du 22 avril dernier, lorsqu'il estime que *« le traitement litigieux comporte des garanties appropriées pour les droits et libertés des personnes concernées et n'institue pas un "dispositif disproportionné" »*.

2. **Présentez les modalités par lesquelles l'autorité judiciaire demande la réquisition d'images de sécurité à des opérateurs. Le processus vous semble-t-il fluide ?**

Ces images sont obtenues par la procédure habituelle des réquisitions, qui dépend donc du cadre d'enquête dans lequel on se trouve : flagrance, enquête préliminaire ou information judiciaire.

Toutefois, compte-tenu de la durée de conservation limitée de ces images de sécurité, il s'agit habituellement d'un acte d'enquête devant intervenir le plus rapidement possible après les faits, ce qui relève le plus souvent de l'enquête de flagrance, permettant aux enquêteurs de requérir directement les images de sécurité sans autorisation du procureur de la République (art. 60-1 CPP).

L'hypothèse d'une réquisition dans le cadre de l'enquête préliminaire impose d'obtenir préalablement l'autorisation du procureur de la République (art. 77-1-1 CPP) qui prend parfois la forme, d'après les retours que nous avons obtenus de nos collègues du parquet, d'une « autorisation générale » pour des raisons de fluidité. Cette pratique apparemment limitée nous semble cependant contestable au regard de l'absence de contrôle de proportionnalité *in concreto* qu'elle induit.

3. **Les images attachées à des communications électroniques sur des messageries privées ou des réseaux sociaux sont-elles aujourd'hui utilisées – et de quelles façons ? – dans des procédures en tant qu'éléments probants ?**

À titre liminaire, en réponse à cette question et aux questions n°5 et suivantes, relatives à la force probante des images ou extraits de video-surveillance, il importe de rappeler que ces éléments de preuve ne dérogent pas aux règles de droit commun de l'administration de la preuve prévues aux articles 427 et suivants du code de procédure pénale : les infractions peuvent être établies par tout mode de preuve et le juge se décide d'après son intime conviction, à condition que les preuves sur lesquelles il la fonde aient été versées aux débats et contradictoirement discutées devant lui.

Ainsi, il est totalement admissible – et cela se pratique assez fréquemment – que les « photos de profil » attachées à des messageries privées ou des réseaux sociaux soient utilisées dans les procédures, notamment lorsqu'il s'agit de faire état de l'activité en ligne d'une personne ou de l'identifier. En l'absence de contestation (par exemple lorsque l'enquête révèle que l'ordinateur est utilisé par plusieurs personnes ou que le compte a été piraté), ce sont des éléments considérés comme probants, notamment en matière de pédo-pornographie ou de proxénétisme (annonces sur des sites spécialisés) ou, de façon plus générale, s'agissant de délits de presse ou commis en ligne (menaces, apologie du terrorisme, etc.). Pour autant, l'image de profil ne permet évidemment pas de s'assurer qu'elle est bien celle du titulaire du compte concerné et il ne pourra donc s'agir que d'un indice de l'identité parmi d'autres.

Enfin, ainsi que cela a été évoqué en réponse à la première question, le fichier TAJ dispose désormais d'une fonctionnalité permettant de tenter un recoupement par reconnaissance faciale entre toute image et l'ensemble des portraits contenus dans le fichier. Il est donc désormais aisé de faire une telle recherche en utilisant une image de profil issue des réseaux sociaux, même si, pour les raisons évoquées précédemment, une telle « identification » n'a de sens qu'à condition de pouvoir établir que la « photo de profil » associée au compte de messagerie est bien la photo de la personne qui utilise ce compte.

4. **Quelle est votre réflexion sur la surveillance vidéo d'une personne placée en garde à vue ? Le cadre légal actuel (loi du 24 janvier 2022) est-il à votre sens satisfaisant, notamment sur les modalités de recueil du consentement de la personne gardée à vue et de déclenchement de l'enregistrement ?**

L'évaluation de ce nouveau cadre légal est difficile dans le mesure où nous n'avons eu aucun retour de collègues dans le ressort desquels ce dispositif aurait déjà été mis en œuvre : l'ensemble des collègues consultés ont ainsi indiqué que, sur leur ressort, les personnes gardées à vue y étaient encore surveillées directement par les enquêteurs sans recours à la vidéosurveillance ou faisaient l'objet d'une vidéo-surveillance systématique.

Il doit être relevé que le décret d'application de ce dispositif n'est manifestement pas encore intervenu, ni l'avis de la CNIL prévu par l'article L. 256-5 du code de la sécurité intérieure. Par ailleurs, la question fait état du recueil du consentement de la personne gardée à vue alors que ce consentement n'est en aucun cas prévu par la loi.

En toute hypothèse, il est d'ores et déjà permis d'observer que ce nouveau cadre légal envisage uniquement la vidéo-surveillance sous l'angle de la prévention de l'évasion ou des menaces que la personne gardée à vue ou en retenue douanière représenterait pour elle-même ou pour autrui. Autrement dit, il est fait totalement abstraction de la prévention des violences dont pourrait faire l'objet la personne gardée à vue, notamment de la part des enquêteurs, ce qui est pourtant, dans la plupart des cas de violences policières poursuivies, un élément de preuve déterminant pour établir les faits. De ce point de vue, l'idée de confier aux services enquêteurs la responsabilité du déclenchement ou de l'arrêt de l'enregistrement ne nous semble pas être la plus pertinente, nonobstant l'ensemble des garanties imaginées pour préserver l'intimité et l'image de la personne gardée à vue, dont il faut convenir qu'elles ont le mérite de combler un vide juridique.

5. **Pouvez-vous objectiver la force probante des images de sécurité captées par des dispositifs de vidéoprotection, des caméras-piétons, des caméras embarquées, des drones, des LAPI ?**

Comme rappelé ci-avant, comme tout élément de preuve, les images devront être confrontées aux autres éléments du dossier et soumises à l'appréciation des parties pour en apprécier la force probante. De même, la force probante dépendra de la qualité des images qu'il est parfois nécessaire de faire expertiser dans les dossiers les plus graves.

Pour un exemple issu des retours obtenus de nos collègues, dans un dossier d'homicide, un mis en cause a été vu sur une vidéo en train de frapper la victime dans une bagarre générale. La victime décèdera à la suite de coups de couteau. Le mis en cause a affirmé qu'il ne possédait pas de couteau et la présence d'un couteau n'était pas évidente sur la vidéo. Une expertise a permis de préciser un peu les circonstances des faits mais la discussion a perduré, le mis en cause affirmant que l'éclat de lumière visible grâce à l'analyse de la vidéo ne venait pas d'un couteau mais des manches de son vêtement.

Cet exemple illustre le fait que la vidéo ne peut faire preuve en elle-même mais peut apporter des éléments au débat. La question demeure toujours celle de la proportionnalité : lorsque l'on cherche à faire la lumière sur des faits, on a toujours la tentation de mettre en œuvre des moyens permettant d'avoir le plus d'informations possibles, pour autant il importe que des limites importantes y soient apportées pour ne pas dériver vers la surveillance généralisée, avec tous les risques démocratiques auxquels elle est associée.

6. **Constatez-vous des conflits d'images ? Par exemple, entre celles prises par un témoin et celles prises par un agent des forces de l'ordre. Avez-vous eu connaissance de manipulations d'images ?**

Non, mais des images différentes peuvent exister en raison des points de vue différents de ceux qui les prennent, et aussi du moment du déclenchement. La meilleure manipulation étant de ne filmer que la partie de la scène favorable à l'intéressé, qu'il soit témoin, victime ou membre des forces de l'ordre. La démarche d'« enquête video » initiée par l'ONG « Index », visant à agglomérer un maximum d'images d'une même scène pour en dresser une reconstitution 3D est, de ce point de vue, assez intéressante en ce qu'elle permet précisément d'éliminer ces conflits d'image voire même la subjectivité de la prise de vue. Plusieurs utilisations en ont été faites dans les médias (Libération), mais pour l'instant, à notre connaissance, il n'est pas encore judiciairement admis que cette technique (qui implique de recueillir des vidéos externes à la procédure) puisse tenir lieu d'expertise.

7. **Les images de sécurité sont-elles régulièrement présentées comme preuves lors des procès ? Est-ce un élément de nature à emporter la conviction des magistrats ou des jurys ?**

Les images de sécurité sont utilisées de façon de plus en plus fréquente, d'où la nécessité d'une véritable réflexion en la matière. Elles doivent néanmoins rester un élément de preuve parmi d'autres, sans valeur intrinsèque supérieure, même si l'on constate que leur force sur l'esprit, donc sur l'intime conviction, peut être plus forte que celle d'un témoignage. La perspective des reconstitutions en 3D de certaines scènes, comme évoqué dans la réponse à la question précédente marquerait d'ailleurs un pas de plus dans l'effet saisissant de ce type d'élément de preuve, laissant l'impression au magistrat ou au juré d'avoir assisté personnellement à la scène qu'il lui appartient de juger.

8. **Comment assurer la régularité des images de sécurité pour garantir leur utilisation dans la procédure pénale ? Les contestations sur la fiabilité des images de sécurité sont-elles fréquentes ?**

L'utilisation des images de sécurité en procédure revient concrètement pour l'enquêteur à dresser un procès-verbal d'exploitation dans lequel il décrit la scène visionnée – ou plus précisément les éléments relatifs aux circonstances de l'infraction – et à joindre au procès-verbal une copie de travail de la vidéo. Compte-tenu de la portée importante donnée à ces procès-verbaux, il est essentiel que la description soit la plus précise et la plus objective possible, pour éviter que la description ne devienne une extrapolation de l'enquêteur.

Sur l'ensemble des magistrats que nous avons pu consulter, aucun n'avait eu l'hypothèse d'une contestation soulevée quant à la régularité des images de sécurité. En revanche, l'exploitation (la description sur procès-verbal) qui en était faite par les enquêteurs était très souvent contestée par les parties, ce qui nécessitait un visionnage en direct par le tribunal, parfois impossible en raison du sous-équipement de certaines salles d'audience, ou encore par le simple fait que le format de la video n'était pas standard et nécessitait un logiciel propriétaire pour la lire.

9. **Dans quelles conditions les images de sécurité prises par des tiers peuvent-elles constituer une preuve en matière pénale**

Les dispositions de l'article 427 du code de procédure pénale énoncent qu'hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve. Le juge doit en outre statuer d'après son intime conviction et fonder sa décision sur les preuves apportées aux débats et soumises à la contradiction des parties. Ce principe de la liberté de la preuve en matière pénale doit

s’accommoder d’un principe de loyauté dans le recueil de la preuve qui ne peut être opposé qu’aux autorités de poursuites. Ainsi, au même titre que les autres catégories de preuve, les images de sécurité restent soumises à ces principes : elles ne disposent d’aucune valeur *infra* ou *supra* probatoire en quelque matière que ce soit et doivent faire, sous la réserve du principe de loyauté, l’objet d’un débat contradictoire.

Au fond, les magistrats privilégient en la matière la notion « d’élément de preuve » : il s’agit de réinscrire la captation dans une appréciation plus générale de « faisceau de preuves convergentes » pour s’assurer de son intérêt probatoire, sans risquer d’ériger l’image en preuve ultime et indépassable, comme cela a pu être relevé au titre d’une réponse précédente.

Qu’elle provienne d’un particulier (téléphone portable, notamment) ou d’un dispositif public, l’image, les circonstances de sa captation (situation d’atteinte à la vie privée par exemple), de sa conservation et de son exploitation doivent pouvoir être questionnées par les juridictions. De cette manière, plusieurs collègues insistent sur l’attention particulière qui doit être portée à la finesse des réquisitions d’extraction ou d’exploitation des images. Il ne s’agit dès lors pas, dans un cas donné, de se limiter à l’indication d’un créneau horaire ou d’un lieu approximatif, mais bien à fournir le maximum d’informations au sein des réquisitions (infractions recherchées, en particulier). L’imprécision des réquisitions constitue ainsi souvent un facteur d’accroissement du temps de recherche, pouvant accentuer la mobilisation de la vidéo surveillance comme enjeu de *« lutte professionnelle »*[5]. Cette imprécision est en outre susceptible d’alimenter la subjectivité de l’image recueillie, dont le recalage contextuel peut être rendu (encore) plus difficile.

Ce dernier point pose également la question de l’hétérogénéité des modalités de recueil des images, hors lieu privé, et des garanties les accompagnant, indissociable de la question générale de la valeur probatoire accordée à l’image.

Ainsi, plusieurs régimes juridiques se superposent, ce qui rend d’ailleurs leur appréhension peu lisible, notamment pour les magistrats du parquet qui y sont souvent confrontés dans le cadre de l’enquête de flagrance. Ce cadre d’enquête, étant souvent associé à un traitement téléphonique en temps réel par le magistrat de permanence, rend difficile les conditions du contrôle du cadre légal par celui-ci et ainsi, de son appréciation de la valeur probatoire des images relatées par le service d’enquête.

En ce qui concerne les images recueillies par les forces de sécurités, hors cadre privé, il convient d’abord de distinguer la vidéo-protection fixe et la vidéo-protection mobile. S’agissant de la première, les dispositions de l'article 226-1 du code pénal interdisent l'emploi d'un procédé quelconque pour capter ou enregistrer l'image d'une personne se trouvant en un lieu privé. L’article L. 251-2 du code de la sécurité intérieure, modifié par la loi n° 2019-773 du 24 juillet 2019, vient toutefois préciser ces dispositions en ce qu’il encadre la transmission et l’enregistrement d’images prises sur la voie publique par le moyen de la vidéoprotection opérée dans les lieux et établissement ouverts au public, comprenant ainsi les lieux et établissements ouverts au public sans autorisation et les propriétés publiques librement ouvertes aux citoyens.

S’agissant de la vidéo-protection mobile, l’article L. 241-1 du code de la sécurité intérieure, modifié par la loi n° 2018-697 du 3 août 2018, en prévoit la possibilité pour les services de gendarmerie, de police nationale et municipale et les sapeurs-pompiers. Enfin, l’article L. 242-5 du code de la sécurité

[5] Dans une contribution au sein de la revue animée par le syndicat, E. Lemaire, sociologue, a pu décrire les interactions intervenant entre différents acteurs, occupant des positions inégales et disposant de ressources inégales dans le processus d’exploitation des données de vidéosurveillance : *« Par exemple, la plupart des membres des services d’enquête estiment que le service vidéo-opérateur n’a pas à connaître les tenants et les aboutissants d’une affaire, car « ce ne sont pas des flics »* ». E. Lemaire « Sommes-nous vidéo-protégé.es ? » in *Délibérée*, n°10, juillet 2020, ed. La découverte, p. 86. https://www.cairn.info/revue-deliberee-2020-2-page-83.htm

intérieure, modifié par la loi n° 2022-52 du 24 janvier 2022 porte sur les caméras installées sur les aéronefs.

Quel que soit le régime applicable, il peut être constaté que les actes de captation vidéo réalisés par les autorités publiques donnent lieu à une jurisprudence moins abondante que les captations audio, étant précisé que ceux-ci se trouvent la plupart du temps légitimés non par un fait justificatif tiré de l'autorisation de la loi mais bien par l'absence d'un des éléments constitutifs du délit d'atteinte à l'intimité de la vie privée (voir notamment Crim. 15 février 2006, n°05-86.969).

Face à la multiplicité de ces modalités de recueils, il nous semble à tout le moins impératif d'opérer une réforme tendant à :

- offrir un régime général unique de garanties des libertés en abrogeant les dispositions dérogatoires du code de la sécurité intérieure pour soumettre l'ensemble des images recueillies et le traitement qui en découle aux dispositions du RGPD et à la loi Informatique & Libertés ;
- permettre la mise en œuvre d'un certificat d'authenticité et d'une information sur les garanties offertes à la personne visée par l'image recueillie par les services d'enquête sous peine d'irrecevabilité devant une juridiction.

10. Est-il fréquent de faire appel à des experts pour interpréter une image de sécurité ou en valider l'authenticité ?

En pratique, le recours à l'expertise s'avère limité et l'on observe plutôt un principe de confiance – aveugle dans certains cas lorsque les moyens matériels des juridictions, le manque d'experts, les délais ou la charge des audiences ne leur permettent pas de visionner elles-mêmes les images – dans la fiabilité du procès-verbal d'exploitation de la vidéo par l'enquêteur.

Lorsque l'enjeu s'y prête, ce type d'expertise pourrait néanmoins avoir un grand intérêt, même s'il convient de mettre en garde contre l'autorité d'une pseudo-scientificité de ce qui ne restera qu'une simple interprétation.

À l'inverse, le développement de savoirs-faire en matière de reconstitution 3D à partir de centaines de captations multiples et variées d'une scène unique (comme cela peut se faire lors de manifestations ; voir *supra,* réponses aux questions n°6 et 7) permet de réduire la marge d'erreur de l'interprétation mais ce savoir-faire reste assez isolé et coûteux.

Enfin, s'il repose sur la multiplicité des sources de captation, cela ne constitue pas un argument pertinent pour démultiplier le nombre de dispositifs de vidéo-surveillance, ce qui serait parfaitement disproportionné par rapport à l'objectif poursuivi.

11. Quel degré d'expertise un magistrat doit-il posséder afin d'exploiter des images de sécurité ?

Une demande de renforcement de la formation en matière de preuve sur le champs spécifique du recueil et du traitement des images numériques a pu être exprimée par nos collègues et nous la partageons. Ceci pourrait d'ailleurs trouver sa place dans la formation initiale des auditeurs de justice et non pas simplement dans le cadre d'une formation continue, investie par les magistrats au gré de leurs changements de fonctions. Pour autant, il convient de remarquer que les magistrats ne maitrisent pas nécessairement le cadre juridique de recueil et d''exploitation des images alors que c'est précisément sur ces points qu'est attendue l'expertise du magistrat (plus que sur l'exploitation des images de sécurité).

L'expertise ne saurait ainsi se limiter à la vérification de l'horodatage et du séquençage des images soumises à son appréciation. La formation qui pourrait être proposée devrait aussi couvrir une large information sur les avancées technologiques et renseigner sur le fonctionnement des groupes prestataires privés chargés de la conception des outils de recueil et de traitement des données.

La question du degré d'expertise des magistrats ne peut toutefois se limiter à la formation. Elle dépend largement des outils mis à sa disposition : les outils aujourd'hui disponibles rendent souvent difficile, voire impossible, la lecture desdites images. Dans le cadre spécifique d'une affaire criminelle, la lecture d'une image doit être encore plus fluide pour être valablement soumise à l'appréciation des jurés. D'une manière générale, le manque de temps dans le traitement d'une affaire renforce la tentation de se contenter des images extraites par les services enquêteurs et de leur traitement.

12. Quelle est votre appréciation de la durée de conservation des images de sécurité ? Est-elle suffisante pour protéger effectivement les droits des justiciables et rechercher efficacement les auteurs des infractions ? Le droit d'opposition est-il effectif ?

Les réactions ayant suivi les incidents survenus au Stade de France le 28 mai 2022, sont sur ce thème intéressantes. La suppression rapide des vidéos de sécurité a été en effet l'un des points cristallisant le débat. Néanmoins, ce cas particulier ne permet pas d'en tirer des généralités sur le droit applicable. En effet, la durée de conservation maximale prévue par les textes est déjà très importante : un mois pour les enregistrements de vidéoprotection sauf réquisition contraire (L. 252-5 du code de la sécurité intérieure), sept jours pour les enregistrements des caméras installées sur des aéronefs, sauf procédure judiciaire, administrative ou disciplinaire (L. 242-4 du code de la sécurité intérieure).

Si cette durée de conservation pourra toujours apparaître insuffisante à certains, le temps judiciaire étant souvent décorrélé de celui de la survenance des faits filmés (dépôt de plainte après l'écoulement des délais de conservation initiaux), prétendre à un allongement des délais de conservation ne résoudra pas cette problématique : peu importe la durée, elle sera toujours trop courte. Par ailleurs, une durée de conservation plus longue romprait tout équilibre relativement à la préservation de la vie privée, sans même évoquer la « rationalisation » de la fonction d'enquêteur, puisque l'enquête doit être pensée dans sa globalité et nécessite théoriquement de nombreux autres actes (auditions, enquêtes de voisinage, surveillance) que l'exploitation massive de vidéos.

Il convient, en outre, d'observer qu'en dépit du temps maximal de conservation, certaines réquisitions ne sont pas satisfaites en raison du fait que la vidéo a été effacée ou est devenue inexploitable, ce qui pose la question fondamentale, quel que soit le temps de conservation maximal, de la qualité de la conservation. Certains des magistrats que nous avons interrogés se sont d'ailleurs résolus à considérer qu'ils ne pourront plus récupérer les images.

Enfin, selon les retours que nous avons obtenus, le droit d'opposition ne fait pas l'objet d'un usage massif, et semble plutôt marginal.

13. Anticipez-vous l'arrivée d'images hypertruquées *(deep fake)* devant les tribunaux ?

Cette hypothèse est présente à l'esprit de nombreux collègues. Pour autant, elle se pose avec moins d'acuité que celle relevant de l'utilisation (recueil et traitement) des données algorithmiques, source d'une véritable inquiétude. La récente diffusion en ligne d'un fichier de notation des allocataires CAF en Gironde n'a fait qu'accentuer cette vive inquiétude. Finalement, l'arrivée de *deep fake* devant les tribunaux ne deviendrait un problème majeur que si la vidéo prenait le rôle de preuve ultime, comme cela se dessine dans l'argumentaire des promoteurs de l'expansion de la vidéo-surveillance.

14. **Les décisions récentes concernant la conservation des données de connexion pourraient-elles nécessiter des évolutions s'agissant de la conservation des images de sécurité ?**

La question des données de connexion et celle des images de sécurité, bien que toutes deux liées à la surveillance de masse, restent juridiquement et concrètement deux sujets qui cheminent à un rythme assez différent : ce n'est pas l'encadrement par le droit interne qui fait défaut dans le cadre de la vidéosurveillance ni la sur-exploitation de celle-ci dans les enquêtes, contrairement à la question des données de connexion. En proportion, l'utilisation des images de sécurité dans les enquêtes semble bien moins importante que l'utilisation des données de connexion – qu'autorise leur conservation beaucoup plus importante, à rebours des préconisations du droit de l'Union européenne, que nous partageons. Il nous semble impératif d'adapter nos pratiques en matière d'utilisation des données de connexion, ainsi que nous y invite la Cour de justice de l'Union européenne et plus récemment la Cour de cassation.

L'évolution de cette problématique touche néanmoins un point plus fondamental car cela met une fois de plus en lumière l'absence d'indépendance et d'impartialité du parquet et l'insuffisance du contrôle judiciaire sur certains actes d'enquête. Le problème de la mise en conformité de nos pratiques avec le droit de l'Union européenne reste toutefois épineux, la saisine d'un juridiction (juge des libertés et de la détention) n'étant pas sérieusement envisageable compte tenu de la masses des demandes, de la lourdeur procédurale et de la charge actuelle des JLD.

15. **Comment appréhendez-vous l'utilisation dans un futur proche de techniques d'intelligence artificielle (caméras augmentées, reconnaissance faciale) couplées à des dispositifs de captation vidéo ? Selon vous, quel encadrement législatif devrait-être mis en oeuvre ?**

Nous nous opposons résolument à cette perspective pour laquelle l'actuel principe de l'interdiction doit être maintenu. Aucune raison sérieuse – même technique, puis que le cadre de la loi Informatique et Libertés permet déjà de s'adapter aux technologies futures – ne nous conduit à envisager une modification du droit applicable à cette matière.

La reconnaissance faciale couplée à des dispositifs de captation vidéo est un traitement de données biométriques, méritant la plus grande rigueur pour les protéger de toute possibilité d'abus des autorités. Bien que cela ne soit pas l'objet de la présente audition, nous appelons d'ailleurs résolument à un rejet de l'article 7 du projet de loi sur les jeux olympiques qui crée une brèche particulièrement inquiétante dans le dispositif existant.