UNIVERSITÉ
CÔTE D'AZUR

Travail de recherche effectué par les étudiants du
Master 2 – Droit Bancaire et FinTech

Pour l'association

HEHOP
HELP FOR HOPE

Sous la direction de : Madame Marina TELLER,
dans le cadre de l'atelier FABLEX
avec l'accompagnement de Julien BONNEL impliqué sur les projets HEHOP,
BlockSY et Blockchain Innov

Septembre 2022

La faculté n'entend donner ni approbation, ni improbation aux opinions émises dans ce travail de recherche. Ces opinions doivent être considérées comme étant propres à leur auteur.

Table des matières

Dans le cadre de l'atelier FABLEX DL4T, projet visant à faire émerger des relations entre le monde universitaire et les entreprises, les étudiants du Master 2 Droit Bancaire et Fintech ont travaillé sur certaines des problématiques rencontrées par l'application créée par l'association HEHOP. Cette application vise à permettre la conservation de preuves de violences conjugales sur blockchain, afin de rendre possible, si la victime le souhaite, leur transmission et leur exploitation par les autorités compétentes.
Cette synthèse reprend le travail des étudiants effectué tout au long de l'année 2021-2022 afin de le rendre exploitable par l'association.
Trois problématiques sont ressorties tout particulièrement et seront par conséquent développées dans cette synthèse : le sujet de la preuve numérique, tant sur les caractéristiques nécessaires à la recevabilité de la preuve que sur le moyen technique de conservation qu'est la Blockchain (I), la protection des données des personnes concernées (II) et les conditions générales d'utilisation du site web de HEHOP (III).

I. Les caractéristiques nécessaires à la recevabilité de la preuve numérique stockée sur blockchain

La preuve pénale est au cœur du procès pénal. En effet, à tous les stades de la procédure se pose le problème de la preuve de l'existence de l'infraction et de la participation de la personne poursuivie à cette infraction. Un des corollaires de la problématique liée à la preuve est le principe de présomption d'innocence fondé par les articles 9 de la DDHC, 6 de la CEDH et de la loi du 15 juin 2000. De fait, la personne suspectée ou poursuivie est présumée innocente jusqu'à ce que la partie adverse ait rapporté la preuve définitive de sa culpabilité.
Le triptyque loyauté, liberté et légalité de la preuve, vise à garantir un certain équilibre afin de protéger les justiciables au cours d'une procédure pénale. C'est ce qui sera discuté au sein de cette partie sur la preuve numérique en se penchant, dans un premier temps sur la recevabilité de la preuve obtenue de manière illicite ou déloyale (1) avant de se demander si le fait d'utiliser la technologie blockchain a un impact sur celle-ci (2).

1. Recevabilité de la preuve obtenue de manière déloyale ou illicite

De plus, l'article 427 alinéa 1 du code de procédure pénale prévoit que les infractions peuvent être établies par tout mode de preuve. Ainsi, c'est le principe de liberté de la preuve qui prévaut en procédure pénale. Néanmoins, un principe de liberté de la preuve absolue ne garantit pas au justiciable que la preuve ait été obtenue de manière juste. C'est pourquoi cette liberté de la preuve est assujettie à deux principes : la légalité et la loyauté dans le mode de preuve. De plus, il est à noter que le juge demeure garant des libertés. En effet, outre les principes de légalité et de loyauté de

la preuve, le principe de liberté de la preuve et notamment celui de l'intime conviction sert également de rempart à des atteintes trop importantes aux garanties des justiciables. Le juge a pour fonction essentielle d'évaluer les preuves qui lui sont soumises.
Si en théorie, les preuves déloyales ou illégales ne peuvent pas être reçues en justice, des lois successives sont venues restreindre ces principes et les altérer pour renforcer les pouvoirs de ceux qui recherchent la vérité. Il est possible de citer la loi Perbenne du 9 mars 2004, la loi du 14 mars 2011, du 25 juillet 2015 et dernièrement la loi sur le terrorisme du 3 juin 2016.

Concernant la validité des preuves obtenues de manière déloyale ou illicite, en matière pénale, la Cour de cassation a jugé dans un arrêt de principe rendu le 7 mars 2012 que celles-ci pouvaient être admises en justice. En effet, aucun article de loi ne permet aux juges d'écarter une telle preuve. De la même manière, les actes comportant des retranscriptions de ces enregistrements audio ne pourront non plus donner lieu à annulation. La limite à ce principe étant le respect des droits fondamentaux de la personne humaine dont l'interdiction de la torture ainsi que l'existence éventuelle, dans le procès pénal, d'une question de droit civil ou commercial soumise à une disposition particulière.

Il convient cependant de se demander si la partie adverse pourrait soulever ***le droit à un procès équitable*** *et si, en avançant une preuve enregistrée à l'insu de la personne concernée, cela ne conduirait pas à une* ***illégalité des armes dans le procès*** *?*

L'article 6 § 1 de la Convention de sauvegarde des droits de l'Homme et des libertés fondamentales prescrit que « *toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle* », c'est le **principe de l'égalité des armes**. Ce principe « implique l'obligation d'offrir à chaque partie une possibilité raisonnable de présenter sa cause - y compris ses preuves - dans des conditions qui ne la placent pas dans une situation de net désavantage par rapport à son adversaire » (CEDH, 27 oct. 1993, Dombo Beheer B.V. c/ Pays Bas, n° 14448/88, § 33 ; voir également : 16 juin 2005, Storck c/ Allemagne, n° 61603/00, § 161).

Si aux premiers abords, on pourrait penser que le fait pour une victime de mettre en avant, lors d'un procès, une preuve obtenue illégalement (en l'espèce par le biais de l'application HeHop) pourrait placer la partie adverse dans une situation de non-égalité dans le cadre du procès, c'est en réalité le contraire.

En effet, le fait pour une partie d'avoir en sa possession une preuve qui pourrait influencer le jugement final en sa faveur, et de ne pas pouvoir mettre en avant cette preuve (obtenue légalement ou non), serait une illégalité des armes. C'est en ce sens

que la Cour de cassation juge, en limitant la portée du droit au respect de la vie privée : « *constitue une atteinte au principe de l'égalité des armes résultant du droit au procès équitable garanti par l'article 6 de la Convention européenne des droits de l'homme* ***le fait d'interdire à une partie de faire la preuve d'un élément de fait essentiel pour le succès de ses prétentions*** *; que par ailleurs, toute atteinte à la vie privée n'est pas interdite, et qu'une telle atteinte peut être justifiée par l'exigence de la protection d'autres intérêts, dont celle des droits de la défense, si elle reste proportionnée au regard des intérêts antinomiques en présence* » (Cass. com., 15 mai 2007, n° 06-10.606, Bull. IV n° 130 ; D. 2007, p. 2775, obs. A. Lepape).

Afin d'analyser un peu plus en détail la jurisprudence en la matière, il peut être intéressant de se pencher sur un arrêt rendu en 2003 par la Cour de Cassation Belge ***dit « Antigone*** ». Cet arrêt admet la recevabilité de la preuve en matière pénale, jusque-là exclue, en établissant des conditions de recevabilité, d'équité et de proportionnalité afin que celle-ci soit admise. Par la suite, plusieurs autres décisions vont suivre dans ce sens. La Cour de cassation, dispose : « u*ne preuve obtenue illégalement est admissible* », toutefois elle ajoute à cette affirmation trois conditions non cumulables. La première condition s'attache à la loi, en effet, la loi ne doit pas prévoir elle-même la sanction de nullité pour l'irrégularité en question. Ainsi si la loi prévoit une nullité sur la preuve irrégulière, celle-ci ne sera pas admissible. La deuxième condition est que rien n'entache la fiabilité de la preuve. Pour finir, la troisième condition est que la preuve ne soit pas contraire au procès équitable. Malgré la consécration des principes énoncés par cette jurisprudence et transposés par le législateur aux termes de l'article 32 du titre préliminaire du Code de l'instruction criminelle, la jurisprudence en la matière n'est pas constante, ce qui crée une insécurité juridique.

En droit français, l'irrégularité de la preuve entraîne une non-admissibilité par les juges.
En 2012 encore il était exprimé par un agent du droit qu'il n'était pas possible de produire des enregistrements en justice car cela constituerait une preuve déloyale et que cela serait irrecevable. En droit pénal, toutefois, l'article 427 du Code de procédure pénale dispose : « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction. Le juge ne peut fonder sa décision que sur des preuves qui lui sont apportées au cours des débats et contradictoirement discutées devant lui.* » Dans cet article, le mode de preuve est qualifié de « *libre* » mais certaines exclusions sont prévues par la loi. Les cas exclus par la loi renvoient à l'arrêt Antigone en 2003 qui n'admettait pas l'irrégularité d'une peine dans le cas où la loi y prévoyait une nullité. A défaut, dans le code de procédure pénale il y a une libre appréciation de la preuve par le juge. Au fil des années plusieurs conditions se sont mises en place, suite à un arrêt de la **Cour de cassation le 7 mars 2012**. Il était déjà admis par la Cour française l'admission de la preuve dans les cas où la production de preuve par les parties « *peut être discutés contradictoirement* ». De surcroît, suite à l'arrêt Bettencourt, le 31 janvier

2012, les juges ont admis que « *les enregistrements audios obtenus à l'insu d'une personne sont recevables en justice en tant que preuve afin de porter plainte contre cette personne au titre d'infractions pénales dont elle se serait rendue coupable et sans que le droit au respect de la vie privée ni même la violation du secret professionnel puisse valablement constituer une limite* ». Les conditions sont strictement encadrées et reflètent les jurisprudences susmentionnées.
Pour finir, dans les affaires pénales tout moyen de preuve est admis, même illicitement produit dès lors qu'il est « produit par un particulier et constitue une pièce à conviction » ***Paris, 8 février.1995***. Il est précisé dans cet arrêt qu'aucune autorité publique ne doit s'immiscer dans la confection de pièces à conviction.

En droit civil la situation diffère quelque peu. En effet, si l'article 1358 du Code civil dispose que « *Hors les cas où la loi en dispose autrement, la preuve peut être apportée par tout moyen* » et que l'article 9 renforce cette idée en expliquant que « *Il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention.* » la preuve illicite est restée jusqu'à peu exclue.
Par un arrêt rendu le 19 novembre 2014, la Chambre sociale de la Cour de cassation refuse d'admettre un mode de preuve déloyale. Cela signifie que dans les cas où la personne n'est pas mise au courant de cet enregistrement, c'est à dire de la création de cette preuve, celle-ci ne peut être acceptée par les juges.
Néanmoins, depuis quelques années la tendance est au changement. En effet, dans le droit du travail, lors d'une affaire portant sur un système de vidéosurveillance illicite, la **Cour de cassation dans un arrêt du 10 novembre 2021,** soc, Réunion (Arrêt n° 1249 FS-B, pourvoi n° 20-12.263, D. 2021. 2093) admet que : « l'illicéité de l'administration de la preuve n'entraîne pas nécessairement » le rejet de celle-ci. Dans la continuité de l'arrêt Antigone, en Belgique, la Cour de cassation va admettre, en France, qu'une preuve dite « irrégulière » ou « illicite » soit admise dans certaines conditions strictement énoncées par la Cour de Cassation.
Premièrement, il y a une condition d'équité : les juges admettent qu'une preuve non équitable ne soit pas recevable. Deuxièmement, le respect de la vie privée doit être pris en compte : le droit à la preuve se limite à un l'accès équitable et proportionnel au but poursuivi. C'est d'ailleurs un principe énoncé par l'arrêt Antigone. Pour finir, la preuve dite irrégulière se doit d'être indispensable à l'exercice de ce droit.
Ce cas d'espèce transpose les conditions émises par la jurisprudence de l'arrêt « Antigone » de 2003 et même si cet arrêt a pour fond un litige en droit du travail, le contentieux concerne la recevabilité de la vidéosurveillance. Un rapprochement peut être fait avec la problématique de la preuve concernant l'application HeHop. En effet, cette dernière donne la possibilité de transmettre des vidéos et des photos à un tiers dans le but de constituer un procès.

Ainsi, il est fort probable, dans le cadre, par exemple, d'un procès où une victime de violence conjugale mettrait en avant des enregistrements obtenus de façon déloyale, que ces derniers ne soient pas refusés par le juge.

En effet, au vu des jurisprudences précitées, nous pensons plutôt que dans l'arbitrage entre le respect du droit à la vie privée et la défense des intérêts d'une victime, ayant en sa possession des preuves essentielles au succès de ses prétentions, le juge ne refusera pas d'admettre ces preuves, même obtenues illégalement ou à l'insu de la personne concernée.

En tout état de cause, He Hop devra mettre en forme une déclaration ou une charte au sein de son application prévoyant la qualité de la personne qui génère la preuve. En effet, si la preuve est entre les mains des OPJ il faudra démontrer que celle-ci a été constituée par la victime, en sa qualité propre.
En outre, la charte devra prévoir que la victime s'engage à admettre contractuellement qu'elle génère et détient la preuve en sa qualité. Une fois que la qualité de l'individu est retenue la preuve pourra être rapportée par n'importe quel moyen y compris films, écoutes, enregistrement comme le propose He Hop.

2. La recevabilité de la preuve numérique stockée sur blockchain

1) L'explication nécessaire du processus de stockage du document dans la Blockchain et le coffre-fort numérique de HeHop

Le document numérique passe par un processus de hachage qui génère son « empreinte », c'est-à-dire d'une suite de chiffres. Cette empreinte est inscrite dans un bloc de la Blockchain.
Pour mieux comprendre le processus, prenons l'exemple d'un contrat qui serait intégré dans une blockchain de cette manière. Le contenu du contrat ne serait pas enregistré sur cette blockchain, seule son empreinte le serait. Or, l'empreinte ne permet pas de reconstituer le contenu du contrat et donc d'en connaître la teneur. En effet, l'empreinte ne permet pas de remonter jusqu'au document car le codage ne peut avoir lieu que dans un sens.
Dans HeHop, l'utilisation d'une Blockchain est couplée à celle d'un coffre-fort numérique. HeHop supprime l'original du document dans le téléphone au moment où son empreinte est transférée dans la blockchain afin de protéger l'utilisateur, puis une copie est générée dans le coffre-fort numérique.
L'intérêt de la Blockchain est de certifier que cette copie a la même empreinte que celle du document l'original qui a été intégrée dans la Blockchain. Celui qui a archivé le document doit détenir une « clé » (un code secret). En procédant à un nouveau codage de la copie dans la blockchain, l'on peut vérifier si l'empreinte générée est identique à celle de l'original. Cela signifiera que la copie du document est conforme à l'original dont il se prévaut. Elle pourra alors être produite en justice.
Ainsi, la valeur probante de la copie dépend de la capacité du juge à comprendre le processus de stockage du document sur Blockchain. Il travaille sur la copie en admettant que cette dernière est conforme à l'originale qui a été codée et archivée dans la blockchain.

2) Le questionnement découlant de la valeur probante d'une copie

La **réforme du droit des obligations** introduite par l'ordonnance n°2016-131 du 10 février 2016 portant **réforme du droit des contrats**, du régime général et de la **preuve des obligations** est entrée en vigueur le 1er octobre dernier. A cette occasion, la réforme a notamment apporté des modifications sur la **preuve** des **obligations**.

Avant le 1er octobre, l'**article 1334** du Code civil disposait que *« les copies, lorsque le titre original subsiste, ne font foi que de ce qui est contenu dans le titre, dont la représentation peut toujours être exigée »*. Le principe était donc que le document original devait toujours pouvoir être produit.

Toutefois, l'**article 1348 du Code civil** prévoyait une exception *« lorsqu'une partie ou le dépositaire n'a pas conservé le titre original et présente une copie qui en est la reproduction non seulement fidèle mais aussi durable. »* Il précisait qu'est *« réputée durable toute reproduction indélébile de l'original qui entraîne une modification irréversible du support ».*

Sur la base de cet article, la question de la force probante des photocopies avait été discutée devant les tribunaux. D'abord reconnue comme simple c**ommencement de preuve par écrit**, elle s'était ensuite vue reconnaître le caractère de **reproduction durable et fidèle** exigé par l'article 1348 du Code civil, avant de **constituer la preuve de l'acte lui-même (Cass. 1ère civ., 25 juin 1996, n°94-11.745)**.

La **réforme du droit des obligations** a introduit un article 1379 consacré aux copies, rédigé comme suit :

Article 1379 : ***"****La copie fiable a la* ***même force probante que l'original.*** *La fiabilité est laissée à l'appréciation du juge. Néanmoins est réputée fiable la copie exécutoire ou authentique d'un écrit authentique.*

Est présumée fiable jusqu'à preuve du contraire *toute copie résultant d'une reproduction à l'identique de la forme et du contenu de l'acte, et dont l'intégrité est garantie dans le temps par un procédé conforme à des conditions fixées par décret en Conseil d'État.*

Si l'original subsiste, sa présentation peut toujours être exigée".

Le décret auquel renvoie ce nouvel article a été publié au Journal Officiel du 6 décembre 2016 (Décret n°2016-1673 du 5 décembre 2016 relatif à la fiabilité des copies et pris en application de l'article 1379 du Code civil).

Il distingue les **copies électroniques** des autres formes de **copies**.

Pour ces dernières, le décret reprend la formulation de l'ancienne rédaction du code civil en exigeant *« un procédé de reproduction qui entraîne une modification irréversible du support de la* ***copie*** *»*. Le nouveau décret ne va donc pas venir modifier la force probante des photocopies.

Il vient par contre **préciser les modalités de reconnaissance des copies électroniques**. Les articles 2 à 6 du décret viennent ainsi détailler les conditions que doivent remplir les copies électroniques pour pouvoir être considérées comme fiables et donc avoir la même force probante que l'original. Parmi ces conditions :

- Le **procédé de copie doit produire des informations liées à la copie, destinées à l'identifier,** en précisant le contexte de la numérisation, en particulier les dates de création de la copie, la qualité du procédé devant être appréciée par des tests et des contrôles.

Ce critère semble rempli puisque le procédé de stockage du document par Hehop est très sécurisé et permet d'horodater l'insertion du document sur la chaîne et donc l'intégration de la copie dans le coffre-fort qui est simultanée.

- Une empreinte électronique doit garantir la détection de tout modification ultérieure, condition présumée remplie en cas notamment d'**horodatage qualifié** ;

Cette condition semble également remplie puisque la technologie Blockchain permet d'attester qu'aucune modification du document n'a pu intervenir à postériori grâce au système de l'empreinte.

- La copie doit être conservée dans des conditions permettant d'éviter son altération, dans sa forme ou son contenu ;

Cette condition est également remplie grâce à l'association de la technologie Blockchain à un coffre-fort numérique qui garantit une conservation optimale de la copie.

- Enfin, l'accès aux dispositifs de reproduction et de conservation décrit ci-dessus doit faire l'objet de mesures de sécurité appropriées et l'ensemble des dispositifs et mesures ci-dessus doit être formalisé dans une documentation conservée aussi longtemps que la copie électronique produite.

II. Le Règlement général sur la protection des données et la Blockchain

Une fois les preuves récoltées, se pose la question de la protection des données personnelles des personnes concernées par ces films, images et enregistrements. Cela pose plusieurs problématiques, notamment en matière de durée de conservation de ces documents (1), de consentement (2), de qualification des acteurs (3), de droit à l'effacement (4), de garantie d'un traitement licite, loyal et transparent (5), et de sécurité et confidentialité des données stockées (6).

1. La question de la durée de conservation de ces documents

Concernant la durée de conservation le RGPD selon la CNIL « les données personnelles ne peuvent être conservées indéfiniment : une durée de conservation doit être déterminée par le responsable de traitement en fonction de l'objectif ayant conduit à la collecte de ces données ». En tant que responsable de traitement, HEHOP devra prévoir une durée de conservation des données pouvant se baser sur la prescription de l'infraction commise par l'agresseur. En effet, une marge d'appréciation est laissée aux responsables de traitement par la loi : aucune durée de principe n'est fixée pour la durée de conservation, le responsable de traitement doit conserver les données uniquement pendant la durée nécessaire à l'accomplissement de ses finalités.

2. La question du consentement

Le consentement est une des obligations imposées par le RGPD afin que le traitement puisse avoir lieu de manière licite. Il est donc nécessaire de recueillir le consentement de la personne faisant l'objet d'un traitement. Pour cela, l'application contient un paramétrage faisant en sorte que la preuve enregistrée par l'utilisateur ne soit pas directement mise sur le coffre-fort et qu'il y ait besoin d'une action positive permettant de consentir à transmettre les éléments. Il pourrait être envisagé une modification de ce système sous accord préalable de la CNIL, afin que lors du premier lancement, un recueil express du consentement ait lieu pour que lors de l'enregistrement de la preuve, elle soit directement transmise dans le coffre-fort sécurisé et qu'il n'y ait plus de risque de suppression de la preuve. Afin de pouvoir revenir sur cette décision et de ne pas bloquer l'utilisateur, il y a la nécessité de laisser une possibilité de désactiver et réactiver ce paramétrage.

3. La question de la qualification des acteurs

L'article 82 du RGPD prévoit une responsabilité du responsable de traitement et du sous-traitant. Dès que le responsable de traitement a participé au traitement, il est responsable du dommage causé par le traitement qui a constitué la violation du RGPD. Par ailleurs, le sous-traitant ne sera tenu responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations qui lui incombent dans le cadre de son activité. Mais il pourra aussi être responsable s'il a agi en dehors des

instructions qu'il a reçues du responsable de traitement. En revanche, le responsable de traitement et le sous-traitant seront exonérés de responsabilités s'ils prouvent que le fait qui a provoqué le dommage ne leurs est pas imputable.

4. La question du droit à l'effacement

Le RGPD en son article 17 octroie un droit à l'effacement aux personnes concernées faisant l'objet d'un traitement de données personnelles (ici, les utilisateurs de HeHop dont les photos, vidéos et enregistrements vocaux sont collectés, stockés puis transmis aux autorités judiciaires). L'exercice d'une telle prérogative n'est pas particulièrement difficile à satisfaire concernant les données liées à l'identification des utilisateurs de HeHop, qu'il conviendra de supprimer s'ils en formulent la demande (mot de passe, e-mail, question secrète). En revanche, les choses se compliquent quant à la suppression définitive des données inscrites sur blockchain, puisque l'effacement remet en question le principe et l'intérêt même de son utilisation. La CNIL, également consciente de ces enjeux, est venue dès 2018 tempérer le droit à l'effacement en cas d'usage de la blockchain. Selon elle, malgré le fait qu'une suppression totale soit techniquement impossible, la "suppression de la clé secrète de la fonction de hachage" a un effet suffisant pour garantir le droit à l'effacement. Il conviendra donc de maintenir cette mesure technique et d'en documenter le processus en cas de contrôle de la CNIL.

5. La garantie d'un traitement licite, loyal et transparent

Selon le RGPD en son article 5 est précisé les différents principes que doivent respecter les responsables de traitements. A savoir les données à caractère personnel doivent être traitées de manière licite, loyale, transparente ; collectées pour des finalités déterminées, explicites et légitimes. Hehop doit prendre en compte le fait que les données collectées doivent être limitées et utiles. De plus, l'application doit vraiment mettre les moyens concernant la sécurisation des données qui est fondamentale dans le domaine qu'elle exerce.

6. L'obligation de sécurité et de confidentialité des données

Le responsable de traitement a une obligation de sécurité et de confidentialité qui découle du règlement général sur la protection des données. Cette obligation implique la mise en place de mesures opérationnelles et organisationnelles afin de garantir la protection des données traitées (article 34 loi informatique et liberté).
Une cartographie des risques est la première étape à faire afin de procéder à un état des lieux des données traitées et des risques qui peuvent être amenés à se réaliser. Durant cette étape, il faut identifier les mesures à mettre en place pour éviter la réalisation du risque.
L'ensemble des mesures mises en place doit être consigné, avec la cartographie des risques, au sein d'un registre des traitements à présenter à la CNIL en cas de contrôle.
Parmi les mesures à mettre en place il faut :

- Une gestion des habilitations des personnes qui ont accès au traitement des données et, une révision régulière de ces habilitations

- Il faut chiffrer les données et utiliser un protocole qui garantit la confidentialité et l'authentification du serveur destinataire pour les transferts de fichiers (SFTP ou HTTPS)
- La formation des salariés sur les thématiques de sécurisation des données est très importante aussi

Il faut garder en tête que le risque est évolutif donc, il est nécessaire d'effectuer des vérifications régulières de l'efficacité de son dispositif de sécurité.

III. Les conditions générales d'utilisations (CGU)

Dans cette dernière partie, seront développées des suggestions concernant les conditions générales d'utilisation de l'application HEHOP.
Le contenu des CGU n'est pas formalisé par la loi, il est laissé à la libre appréciation de l'éditeur.

- Dans l'onglet « responsabilité », faire une partie sur la dénonciation calomnieuse et y écrire :

« La dénonciation d'un fait de violence conjugale que l'on sait faux ou partiellement inexact, lorsqu'elle est adressée soit à un officier de justice ou de police administrative ou judiciaire, soit à une autorité ayant le pouvoir d'y donner suite ou de saisir l'autorité compétente, soit aux supérieurs hiérarchiques ou à l'employeur de la personne dénoncée est punie de cinq ans d'emprisonnement et de 45 000 euros d'amende ».
« La responsabilité de He hop ne peut en aucun cas être engagée pour une dénonciation calomnieuse de la part d'un utilisateur. En effet He Hop ne peut pas évaluer l'exactitude des données transmises aux autorités ».

- Préciser également sur l'hypothèse d'une utilisation détournée (dans un but de dissuasion) :

« L'application HEHOP doit être exclusivement utilisée pour recueillir des preuves d'un fait de violence conjugale. Toute utilisation détournée pourra faire l'objet de poursuites ».

- Le cas de figure de l'utilisation de HeHop par un tiers : enfant, ami, parent, voisin

L'hypothèse qu'un tiers puisse filmer, via HeHop, une agression est un élément important qui doit être pris en compte dans les conditions générales d'utilisations. Ces dernières devront informer ces tiers qui auront des règles spécifiques. En effet, les preuves qui seront enregistrées constituent des données personnelles liées à la victime et à l'agresseur. Le RGPD prévoit que le consentement est nécessaire pour collecter des données, ce qui dans le cadre de violence paraît peu faisable. Néanmoins, le RGPD assouplit cette règle car il est prévu qu'une absence de consentement puisse être justifiée dès lors que le traitement de la donnée a un intérêt légitime. Ce dernier est un élément important, il serait intéressant de rappeler et d'insister dans les CGU sur cette notion d'intérêt légitime qui est de constituer une preuve pénale pour la victime et de préciser que tout autre finalité serait un détournement (cf partie sur la dénonciation calomnieuse).
L'article 77-1-1 du Code de procédure pénale dispose que le procureur de la République est en droit de réquisitionner des preuves, même celles qui découlent d'un traitement de données nominatives ou issues d'un système informatique. De ce fait, il serait envisageable de prévenir les tiers via les CGU que les preuves récoltées pourront faire l'objet d'une réquisition, sans possibilité de s'opposer à celle-ci.

Néanmoins, le Conseil constitutionnel a déclaré que cette disposition législative n'était pas conforme constitutionnellement lors d'une QPC du 3 décembre 2021 (décision n°2021-952 QPC). Cette loi devra être abrogée au plus tard le 31 décembre 2022. Il a été indiqué que cette abrogation n'aura pas d'effet rétroactif, ce qui signifie que les preuves réquisitionnées avant l'abrogation de cet article, ne seront pas remises en cause.

En d'autres termes, il faudra indiquer la possibilité d'une réquisition de preuve mais il faudra se tenir à jour et réadapter les CGU selon les nouvelles règles qui seront applicables à ce sujet.

- Atteinte à l'intimité et au respect de la vie privée :

Le Code pénal sanctionne, à l'article 226-1 du Code pénal, d'une peine « d'un an d'emprisonnement et de 45.000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui :

  - 1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;
  - 2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé »

L'article 226-2 du Code pénal ajoute que sont punies des mêmes peines le fait de : « Conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1 du Code pénal ».

L'article ajoute que, « lorsque l'infraction est commise par la presse écrite ou audiovisuelle », la détermination des personnes responsables résulte, pour la presse, de l'article 42 de la loi du 29 juillet 1881 sur la liberté de la presse, et pour l'audiovisuel, de l'article 93-3 de la loi du 29 juillet 1982 sur la communication audiovisuelle qui prévoient une responsabilité pénale " en cascade ".

Pour finir, l'article 226-3 du Code pénal prévoit une peine de « cinq ans d'emprisonnement et de 300.000 € d'amende » est encourue pour :

« La fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente d'appareils ou de dispositifs techniques » conçus pour réaliser les actes prévus par l'article 226-1 du Code pénal.

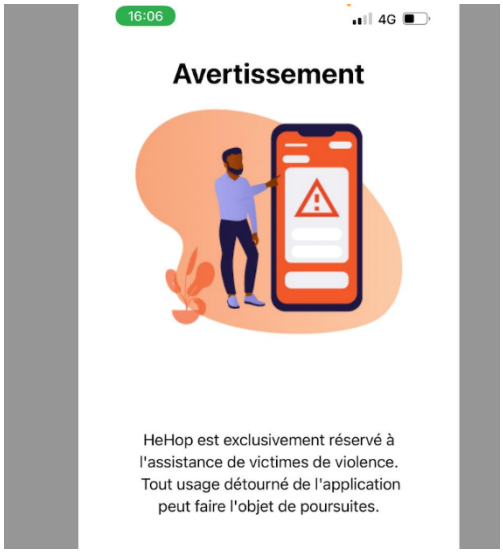
Il faut donc que les utilisateurs sachent qu'ils portent atteinte à l'intimité et au respect de la vie privée d'autrui et que cela ne peut se faire que dans le cadre du recueil d'éléments de preuves de la survenance de violences conjugales, de manière proportionnée et limitée.

- Suggestion de slides explicatives à ajouter :

1ere slide Dénonciation calomnieuse / Usage détourné : C'est un délit puni de cinq ans d'emprisonnement et de 45.000 euros d'amende.

Elle consiste à dénoncer le prétendu auteur d'un fait que l'on sait inexact. Elle constitue une atteinte à l'honneur sanctionnable au regard des articles 226-10 à 226-12 du Code pénal

- *2ème slide Usage détourné :* « L'application Hehop doit être exclusivement utilisée pour recueillir des preuves d'un fait de violence conjugale. Toute utilisation détournée pourra faire l'objet de poursuites ».
- *3ème slide pour rassurer l'utilisateur* : explication de ce qu'est une donnée personnelle, de ce qu'est la collecte de celles-ci et exposé des mesures mises en place pour veiller à la protection des données de l'utilisateur.
  Exemple de phrase de conclusion de cette slide : « Les éléments enregistrés sur l'application Hehop ne pourront être utilisés à d'autres fins que celles de permettre de vous mettre en sécurité ».
- *4ème slide* : Pop-up à compléter par « poursuites judiciaires »



- *5ème slide Utilisation d'HeHop par des tiers* : Il faudra indiquer la possibilité d'une réquisition de preuve mais il faudra se tenir à jour et réadapter les CGU selon les nouvelles règles qui seront applicables à ce sujet.