R E P U B L I Q U E F R A N C A I S E

MINISTERE DE LA JUSTICE

DIRECTION DES SERVICES JUDICIAIRES

SOUS-DIRECTION DES FINANCES, DE L'IMMOBILIER ET DE LA PERFORMANCE

Bureau des frais de justice et de l'optimisation de la dépense (FIP4)

N° téléphone : 01.70.22.86.14
N° télécopie : 01.70.22.85.53

Paris, le 13 décembre 2018

Circulaire ☐ Note ☒
Date d'application : immédiate

La garde des sceaux, ministre de la justice

à

Mesdames et Messieurs les premiers présidents des cours d'appel
Mesdames et Messieurs les procureurs généraux près les cours d'appel
(Pour attribution)
Mesdames et Messieurs les référents frais de justice
(Pour information)

N° NOTE : SJ18 – 393 – FIP4 / 13.12.2018

Référence de classement:

Mots clés : Frais de justice – Expertise informatique

Titre détaillé : Note d'information concernant la rationalisation des prestations d'expertises informatiques et d'investigations numériques

Publication : non ☒ si oui B.O. ☐ J.O ☐
INTRANET ☒ *permanente* ☒ *temporaire jusqu'au :*

Modalités de diffusion
Diffusion assurée par la Direction des Services Judiciaires
Bureau des frais de justice et de l'optimisation de la dépense (FIP4)

Pièce jointe : note proprement dite

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE LA JUSTICE

DIRECTION DES SERVICES JUDICIAIRES

LE DIRECTEUR

Paris, le 13 DEC. 2018

La garde des sceaux, ministre de la justice

à

Mesdames et messieurs les premiers présidents des cours d'appel
et

Mesdames et messieurs les procureurs généraux près lesdites cours

pour attribution

Mesdames et messieurs les référents frais de justice

pour information

Objet : Note d'information concernant la rationalisation des prestations d'expertises informatiques et d'investigations numériques.

Pièce jointe : Tableau « *Temps observés en 2017 – Investigations numériques en expertise pénale* ».

Depuis 2015, le bureau des frais de justice et de l'optimisation de la dépense (FIP4) a entamé plusieurs cycles de négociation avec les prestataires, et notamment les experts de justice, pour élaborer, segment par segment, des stratégies d'achat dépassant la simple négociation de gré à gré. Ainsi, la tarification (analyse toxicologique), l'appel d'offre (analyse génétique des individus – FNAEG) ont pu constituer des leviers efficaces.

En décembre 2016, les « *investigations numériques* », identifiées comme un segment présentant un enjeu stratégique, faisaient l'objet de la mise en œuvre d'une « *stratégie achat* ». En effet, il était régulièrement mis en avant par les juridictions les difficultés inhérentes à la pénurie d'experts et à la dépendance vis-à-vis de quelques experts en position quasi monopolistique ainsi que l'enjeu lié tant à la qualité des expertises judiciaires qu'aux délais de traitement desdites expertises.

13, place Vendôme – 75042 Paris Cedex 01
Téléphone : 01 44 77 60 60
www.justice.gouv.fr

En volume de dépense, elles représentent depuis trois années un montant compris entre 8 et 10,5 millions d'euros[1].

Parmi les difficultés remontées, plusieurs magistrats mettaient en exergue la difficulté à analyser les devis et à appréhender les prestations effectivement réalisées par les experts diligentés dans le cadre d'expertises informatiques portant sur tous types de supports numériques (ordinateur, disque dur, smartphone, etc…). Il a dès lors semblé nécessaire de proposer un outil permettant aux magistrats du parquet et aux magistrats instructeurs d'avoir une meilleure compréhension tant des prestations effectivement réalisées par les experts que des prix proposés.

Dans ce contexte, la direction des services judiciaires s'est rapprochée de la compagnie nationale des experts de justice en informatique et techniques associées (CNEJITA).

Le tableau comparatif des volumes horaires de chaque prestation possible en matière d'investigations numériques est le résultat de ce dialogue concerté. Fruit d'un recensement auprès des principales sociétés spécialisées et avec le concours de la Compagnie Nationale des Experts de Justice en Informatique et Techniques Associées (CNEJITA), ce tableau constitue un outil d'aide à la décision afin de permettre à chaque magistrat d'opérer un choix éclairé des experts et d'analyser les devis reçus lors d'une enquête.

Les temps indiqués ont été établis selon un matériel standard et d'usage courant, sans protection d'accès ni chiffrement. Ils intègrent la réalisation de missions standards et, pour chaque analyse, la rédaction et la fourniture d'un rapport et de ses annexes. Toutefois, ne sont pas inclus :

- les déplacements, le transport des scellés ou des supports de copie numérique ;
- la fourniture des supports de copie numérique ;
- les débours (réquisition opérateur téléphonique, réparation, déverrouillage, etc…) ;
- l'intervention de sociétés spécialisées.

Il convient de préciser que, parmi les prestataires usuels, l'Institut de Recherche Criminelle de la Gendarmerie Nationale (IRCGN) ne procède pas par décompte d'heures mais par un système de forfait. Les volumes horaires de l'IRCGN n'ont donc pas été inclus dans le tableau élaboré.

Pour mieux vous guider dans l'utilisation opérationnelle du tableau, il est utile de préciser les points suivants :

- les temps indiqués dans la colonne CNEJITA constituent des temps de références garantissant une expertise de qualité ;
- certains supports numériques peuvent présenter des volumes conséquents ou une complexité particulière pour extraire les données, ce qui a une incidence sur les devis ;
- la fourchette haute représente un point d'alerte lors de l'examen du devis ;
- lorsque le nombre d'heures indiqué dans le devis dépasse le plafond, il est nécessaire de contacter l'expert pour solliciter des précisions à même de justifier ce dépassement ;
- la moyenne est indicative.

J'attacherai du prix à ce que cet outil d'une part soit largement diffusé auprès des magistrats de votre ressort et particulièrement auprès des magistrats du parquet et des magistrats instructeurs,

[1] Le référentiel d'activité permet depuis 2016 d'identifier les « investigations numériques » réparties entre deux postes :
- Le poste « investigations numériques » (flux 1) représentant environ 8 millions d'euros par année ;
- Le poste « examens techniques et autres expertises » (flux 4) représentant environ 2,5 millions d'euros par année. Il comporte notamment des expertises diverses (informatiques, expertises sur véhicules, etc…).

et, d'autre part, soit systématiquement utilisé dans le cadre des réquisitions ou ordonnances en matière d'expertises informatiques.

Vous voudrez bien me tenir informé, sous le timbre du bureau des frais de justice et de l'optimisation de la dépense, de l'application de ces orientations et des améliorations que vos services seraient à même de proposer.

Le directeur des services judiciaires
Simane GHALEH-MARZBAN

Temps observés en 2017
Investigations numériques en expertise pénale

Matériel standard et d'usage courant, sans protection d'accès ni chiffrement et en état de fonctionnement

Ces temps comprennent :

- La réalisation de missions standards
- Pour les analyses : la rédaction et la fourniture du rapport et de ses annexes

Ces temps ne comprennent pas :

- Les déplacements, le transport des scellés ou des supports de copie numérique
- La fourniture des supports de copie numérique
- Les débours (réquisition opérateur téléphonique, réparation, déverrouillage ...)
- L'intervention de sociétés spécialisées

Analyse de support numérique (inclus l'extraction ou le clonage)	CNEJITA Expert	Fourchette basse	Fourchette haute	Moyenne
Ordinateur de type personnel avec un seul disque dur ou son disque dur système déjà extrait ou le clone de son disque dur système *Les temps d'analyse du disque dur d'un ordinateur sont tributaires, non exhaustivement ,de la capacité du disque, du temps d'utilisation , du nombre d'applications ou outils installés, du système d'exploitation et de sa version.* *Le cryptage de certains disques peuvent nécessiter des opérations préalables, voire de faire appel à un services spécialisés.* *Certains disques peuvent contenir des images virtuelles d'un ou plusieurs autres systèmes d'exploitation (un ordinateur peut faire fonctionner virtuellement plusieurs « ordinateurs » virtuels)* *Dans ce cas cela revient à analyser plusieurs ordinateurs avec le même disque.*	**10 à 20 h**	**3 h**	**27 h**	**15,4 h**
• Temps moyens d'analyse du support				
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	2 h	1,3 h
2. Préparation : Clonage / Mise en œuvre d'outils	1 h	1 h	2 h	1,3 h
3. Analyse et Rapport	8 à 18 h	1 h	25 h	13,9 h
• Cas simplifié (disque absent ou inexploitable, ordinateur peu utilisé, recherche de quelques documents, mission simplifiée ...)	2 à 9 h	1 h	20 h	7,2 h
• Cas complexe (données en très grand nombre, mission complexe ...)	21 à 25 h	21 h	39 h	26,3 h
Disque dur interne supplémentaire ou externe sans système d'exploitation, *Les disques durs internes ou externes contiennent généralement des données : images, vidéos, documents. Ces disques peuvent également contenir des sauvegardes de différents ordinateurs impliquant des analyses de type « disque de système d'exploitation » de nombreux artefacts afférents.* *Les disques de données peuvent contenir des archives (données copiées une fois et stockées pour une durée de plusieurs années. Mais ces disques peuvent également contenir des sauvegardes régulières nécessitant des recherches d'informations dans les secteurs effacés.*	**5 à 13 h**	**3 h**	**22 h**	**12,3 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	0 à 1 h	1 h	2 h	1 h
2. Préparation : Clonage / Mise en œuvre d'outils	1 h	1 h	2 h	1,3 h
3. Analyse et Rapport	3 à 11 h	1 h	20 h	9,6 h
Téléphone simple avec ou sans carte SIM et carte mémoire supporté par un outil spécialisé du commerce sans réparation ni accès direct aux composants internes *Un téléphone simple n'a la possibilité que de téléphoner (journaux d'appels), échanger des SMS (stockage limité) éventuellement de prendre quelques photos, écouter de la musique ou radio . Ce type de téléphone n'a pas accès aux applications de données 3, 4 ou 5G et un accès limité au réseau de données basique GPRS.*	**5 à 7 h**	**3 h**	**11 h**	**6,2 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	2 h	1,3 h
2. Préparation : Extraction données / Mise en œuvre d'outils	0,5 h	1 h	1 h	0,8 h
3. Analyse et Rapport	3,5 à 5,5 h	1 h	9 h	5 h
Smartphone ou Tablette avec ou sans carte SIM et carte mémoire, supporté par un outil spécialisé du commerce sans réparation ni accès direct aux composants internes *Les smartphones et les tablettes ont les possibilités de communication des téléphones simples, mais disposent de toutes les applications d'échanges directs ou sur réseaux sociaux, consultations /multimedia par les réseaux rapides de données 3, 4 ou 5G* *Ils disposent de plus en plus des fonctionnalités et la puissance d'un ordinateur.* *Ils disposent de moyens de localisation très variés (enregistrements GPS, bornage, wifi, media...)* *Ils disposent de capacités de stockage importants* *Les analyses apparaissent de plus en plus pénalisées par des niveaux de sécurité d'accès et le cryptage.*	**10 à 15 h**	**3 h**	**20 h**	**12,3 h**
• Temps moyens d'analyse du support				
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	2 h	1,3 h
2. Préparation : Extraction données / Mise en œuvre d'outils	1 à 1,5 h	1 h	2 h	1,3 h
3. Analyse et Rapport	8 à 13 h	1 h	20 h	10,8 h
• Cas simplifié (appareil peu utilisé, recherche de quelques documents ou des seuls SMS, mission simplifiée ...)	5 à 9 h	1 h	10 h	6,5 h
• Cas complexe (données en très grand nombre, nécessité de saisie manuelle complémentaire, rétroanalyse application non supportée, analyse fichiers techniques, mission complexe ...)	16 à 20 h	13 h	20 h	16,5 h
Téléphone ou Smartphone ou Tablette **avec réparation et/ou autres cas non exploitables par outils courants** *Ces traitements ou analyses concerne des équipements en panne ou bloqués volontairement ou involontairement : pannes, casses ou séjour dans l'eau, écrasés, brûlés ...* *Différentes techniques permettent d'accéder directement au contenu du composant mémoire. Ce composant mémoire monolithique peut supporter des agressions importantes sans se détériorer.* *Toutefois il est sensible aux agressions électriques* *L'analyse peut être rendue difficile en cas de cryptage interne.*	**12 à 25 h**	**3 h**	**25 h**	**16 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Extraction données / Mise en œuvre d'outils	3 à 4 h	1 h	4 h	3,2 h
3. Analyse et Rapport	8 à 20 h	1 h	20 h	12,2 h
Clé USB / Carte mémoire / CD / DVD non protégé et non chiffré *Les données contenues dans ces composants peuvent être variées. Les données effacées peuvent être retrouvées dans des conditions particulières qui peuvent dépendre du mode de gestion interne des données.*	**2 à 6 h**	**2 h**	**10 h**	**6 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Clonage / Mise en œuvre d'outils	0,5 h	1 h	1 h	0,3 h
3. Analyse et Rapport	0,5 à 4,5 h	1 h	8 h	3,2 h

Carte SIM non verrouillée ou avec son code PIN / PUK *Les cartes SIM contiennent principalement les données de gestion d'abonné et d'accès au fournisseur téléphonique.* *Sur les téléphones basiques elles contiennent dans leur espace mémoire très limité une partie de l'activité du téléphone (journaux d'appels, SMS, annuaire ..)* *Sur les smartphones, cet espace mémoire n'est quasiment plus utilisé exploité par le système*	**1 h**	**1 h**	**2 h**	**1,3 h**
Extraction ou copie de données SANS ANALYSE				
Disque dur non protégé et non chiffré	**2 à 4 h**	**2 h**	**6 h**	**3,3 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Travaux : Support destinataire / Clonage	1 à 3 h	1 h	5 h	2,3 h
Téléphone / Smartphone / Tablette supporté par un outil spécialisé du commerce, non verrouillé et non chiffré	**2 à 5 h**	**2 h**	**6 h**	**4,5 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	3,3 h
2. Travaux : Support destinataire / Extraction	1 à 4 h	1 h	5 h	2,7 h
Clé USB / Carte mémoire / CD / DVD non protégé et non chiffré (selon taille)	**1 à 2 h**	**1 h**	**10 h**	**4 h**
Analyse d'objet numérique				
GPS individuel ou balise de géolocalisation *Certains GPS de voiture peuvent disposer de fonctionnalités autres que la géolocalisation : Données de connexion de type GSM voire des applicatifs multimedia.*	**3 à 15 h**	**3 h**	**20 h**	**12,3 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Extraction données / Mise en œuvre d'outils	1 à 7 h	1 h	7 h	3 h
3. Analyse et Rapport	1 à 7 h	1 h	16 h	5,5 h
Box d'opérateur contenant un support de stockage interne *Les Box peuvent contenir des unités de stockage, internes ou externes qui permettent un partage de ces données sur le réseau privé ou sur le réseau public Internet* *L'analyse se rapproche d'une analyse de disque externe* *Certaines box contiennent des journaux plus ou moins importants traçant l'activité de type firewall.*	**5 à 10 h**	**3 h**	**22 h**	**12,5 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Clonage / Mise en œuvre d'outils	1 h	1 h	1 h	1 h
3. Analyse et Rapport	3 à 8 h	1 h	20 h	7,2 h
Console de jeux non protégé et non chiffré	**5 à 10 h**	**5 h**	**16 h**	**19,5 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Clonage / Mise en œuvre d'outils	1 h	1 h	6 h	1,8 h
3. Analyse et Rapport	3 à 8 h	3 h	9 h	5,8 h
Skimmer *Un skimmer est un équipement d'interface permettant de filtrer un accès (Carte à puce, lecteur digicod, clavier ...). Suivant le modèle il peut-être un simple lecteur de carte ou un équipement de lecture avec toutes les possibilités d'un ordinateur.*	**15 à 20 h**	**7 h**	**32 h**	**21,5 h**
1. Administratif : Gestion du scellé / Devis / NEJ / Chorus	1 h	1 h	1 h	1 h
2. Préparation : Extraction données / Mise en œuvre d'outils	3 à 4 h	2 h	13 h	4,8 h
3. Analyse et Rapport	11 à 15 h	4 h	16 h	12 h
Machine à sous ou Caisse enregistreuse *Ordinateur dédié*	**10 à 35 h**	**10 h**	**40 h**	**31,3 h**
Appareil de vidéosurveillance	**15 à 20 h**	**15 h**	**20 h**	**17,5 h**
Analyse et amélioration de photo et de vidéo	**5 à 20 h**	**4 h**	**20 h**	**12,5 h**
Assistance à enquêteur	**4 à 8 h**			
Serveur d'entreprise selon mission et volume de données	devis spécifique			
Autres opérations	devis spécifique			