La surveillance secrète de l'employé

De la protection des données à la procédure pénale

Alexandre Guisan, greffier-juriste (Genève),* et Célian Hirsch, avocat (Genève)**

En cas de soupçons de la commission d'une infraction pénale par un employé, l'employeur peut être tenté de recourir à divers moyens de surveillance. À l'aune de la jurisprudence récente, l'article examine les conditions de la licéité de la récolte de preuve au sein de l'entreprise, puis les conditions de leur exploitabilité, en particulier lorsque la récolte des preuves était illicite. Les auteurs analysent enfin la question du recours à un détective privé ou à l'enregistrement par une dashcam, qui a fait l'objet d'un arrêt récent du Tribunal fédéral. P.P.

Falls der Verdacht besteht, ein Arbeitnehmer habe eine Straftat begangen, kann der Arbeitgeber versucht sein, auf verschiedene Mittel der Überwachung zurückzugreifen. In Anbetracht der jüngsten Rechtsprechung prüft der Beitrag die Bedingungen der Rechtmässigkeit der Beweissammlung im Rahmen des Unternehmens sowie jene ihrer Verwertbarkeit vor Gericht, insbesondere, wenn die Sammlung der Beweise unzulässig war. Die Autoren analysieren schliesslich die Frage der Inanspruchnahme eines Privatdetektivs oder der Aufzeichnung durch eine Dashcam, die Gegenstand eines kürzlich ergangenen Urteils des Bundesgerichts gewesen ist.

I. Introduction

Lorsqu'il soupçonne un employé d'avoir commis une infraction pénale, par exemple un vol dans la caisse, l'employeur peut être tenté d'avoir recours à des mesures de surveillance secrètes afin d'en avoir le cœur net. L'exemple classique est celui de la vidéosurveillance sur le lieu de travail : dans un arrêt récemment publié aux ATF 145 IV 42, le Tribunal fédéral a dû rappeler qu'une telle surveillance, installée par la police avec l'accord de l'employeur, constituait une mesure de contrainte dont le résultat devait être frappé d'inexploitabilité, faute d'autorisation par le Tribunal des mesures de contrainte[1].

La question qui vient naturellement à la lecture de cet arrêt est de savoir si l'employeur bien conseillé n'aurait pas mieux fait de procéder directement à l'enregistrement litigieux, sans l'aide des autorités pénales, puis de remettre les images à ces dernières[2].

La problématique dépasse d'ailleurs la seule vidéosurveillance, puisque l'employeur aura à sa disposition une large palette de mesures, allant de la consultation des données de connexion à Internet de ses employés à la surveillance à distance de leurs téléphones de fonction, en passant par l'utilisation de logiciels-espions enregistrant en temps réel l'entier

* *Alexandre Guisan* est titulaire du brevet d'avocat, greffier-juriste à la Cour de Justice du canton de Genève et doctorant à l'Université de Lausanne.

** *Célian Hirsch* est avocat et assistant doctorant au Centre de droit bancaire et financier à l'Université de Genève.

1 Résumé par *Célian Hirsch,* L'inexploitabilité de la vidéosurveillance d'employés par la police, <www.lawinside.ch/711/> consulté le 23.10.2019 ; pour un commentaire : *Stefan Maeder/Marcus Stadler,* Strafprozessuale Videoüberwachung und informationelle Selbstbestimmung – Anmerkungen zu BGE 145 IV 42, forumpoenale (FP) 5/2 019 396 ss.

2 Pour un exemple récent au niveau européen : CourEDH (Grande Chambre) *López Ribalda et autres c. Espagne,* 17.10.2019, nº 1874/13 et 8567/13 ; au niveau genevois : CJ GE, ACPR/96/2019 du 30.1.2019.

de leurs actions, voire, au vu de l'actualité récente[3], la mise en place d'une filature de ses (ex-)employés.

Ces diverses mesures de surveillance sont surtout l'occasion de revenir sur le régime juridique applicable, en procédure pénale, aux preuves récoltées par des particuliers, lequel implique, dans un premier temps, l'examen du caractère licite desdites preuves, à l'aune notamment de la législation en matière de protection des données. Si les moyens de preuves devaient être qualifiés d'illicites, se posera ensuite la question de leur exploitabilité dans une procédure pénale, qui sera l'objet d'une seconde partie. Enfin, nous reviendrons avec un regard critique sur deux arrêts récents du Tribunal fédéral, l'un sur l'observation par des détectives privés, l'autre sur la *Dashcam,* qui viennent bouleverser le système en place.

II. La licéité de la surveillance lors de soupçons d'infractions pénales

Confronté à une preuve recueillie par un particulier, la première question que doit se poser le juge – pénal, civil comme administratif – est celle de sa *licéité.* En effet, si la preuve devait être qualifiée de licite, elle sera pleinement exploitable[4].

Afin de déterminer le caractère licite du moyen de preuve, il convient de prendre en considération toutes les normes de droit matériel qui lient les particuliers[5]. Les droits procéduraux[6] ainsi que les obligations contractuelles n'en font pas partie[7]. L'illicéité de la preuve peut également découler d'une violation d'une norme de droit étranger[8], mais pas des droits fondamentaux, puisque ceux-ci ne s'appliquent en principe pas aux relations entre particuliers[9]. Néanmoins, la protection des droits de la personnalité permettra de pallier, dans une certaine mesure, l'absence de l'application des droits fondamentaux[10].

A. Le cadre légal pertinent des mesures de surveillance

L'employeur qui soupçonne l'un de ses employés de commettre une infraction pénale et souhaite mettre en place une mesure de surveillance n'en reste pas moins tenu de respecter l'ordre juridique. Trois groupes de normes peuvent entrer en considération dans ce cadre.

Premièrement, l'employeur doit s'abstenir de commettre lui-même une *infraction pénale* lorsqu'il déploie des moyens de surveillance à l'encontre de ses employés. Il ne saurait en particulier surveiller un fait relevant du domaine secret ou privé de l'employé au sens des art. 179 ss CP[11]. On pense également à l'accès indu à un système informatique (art. 143[bis] CP), en lien par exemple avec la surveillance d'un compte e-mail privé de l'employé[12].

Deuxièmement, la surveillance mise en place par l'employeur ne doit pas porter atteinte à la *santé* des employés concernés, que protège notamment l'art. 26 OLT 3, disposition qui interdit l'utilisation de systèmes de surveillance ou de contrôle destinés à surveiller le comportement des travailleurs à leur poste de travail (al. 1) ; lorsque des systèmes de surveillance ou de contrôle sont nécessaires pour d'autres raisons, ils doivent notamment être conçus et disposés de façon à ne pas porter atteinte à la santé et à la liberté de mouvement des travailleurs (al. 2)[13].

---

3 *Credit Suisse aurait fait surveiller un de ses anciens directeurs,* article du Temps publié le 23.9.2019, <https://www.letemps.ch/economie/credit-suisse-aurait-surveiller-un-anciens-directeurs>.

4 Pour un rappel récent, cf. TF 6B_741/2019 du 21.8.2019 cons. 5.2 : « Rechtmässig von Privaten erlangte Beweismittel sind ohne Einschränkung verwertbar ».

5 *Caroline Guhl,* Trotz rechtswidrig beschaffter Beweise zum einem gerechten Straf- und Zivilurteil, Zurich/Saint-Gall 2018, N 229 ; *Benoît Chappuis,* Les moyens de preuve collectés de façon illicite ou produits de façon irrégulière, in : Franz Werro/Pascal Pichonnaz (éds), Le procès en responsabilité civile, Berne 2011, 126 ss, 112 ; *Jürgen Brönnimann,* in : Berner Kommentar, Schweizerische Zivilprozessordnung, 2012, art. 152 CPC N 45 ; *Louis Gaillard,* Le sort des preuves illicites dans le procès civil, SJ 1998 652.

6 *Guhl* (n. 5) N 222 et 245 s. ; *contra Chappuis* (n. 4) 132 ss.

7 Une preuve recueillie en violation d'un contrat, même si celui-ci contient expressément une clause de confidentialité, n'est pas illicite, à moins que la confidentialité résulte de la loi : *Guhl* (n. 5) N 232.

8 En matière de surveillance d'employés, la question du respect du Règlement général sur la protection des données (RGPD ; Règlement [UE] 2016/679) en Suisse pourrait se poser, dès lors que le RGPD connaît une certaine application extraterritoriale : cf. notamment *Yaniv Benhamou/Emilie Jacot-Guillarmod,* GDPR on the Swiss Territory, Jusletter IT 24.5.2018.

9 TF 6B_1241/2016 du 17.7.2017 cons. 1.2.1 ; *Guhl* (n. 5) N 248 ; *Célian Hirsch,* Les observations illicites sont-elles exploitables ?, Jusletter 19.2.2018, N 85 ss ; *contra* ATF 143 IV 387 précisément critiqué ci-dessous cf. *infra* IV).

10 *Guhl* (n. 5) N 249 ; *Chappuis* (n. 5) 122 ss.

11 *Sylvain Métille,* La surveillance électronique des employés, in : Jean-Philippe Dunand/ Pascal Mahon (éds), Internet au travail, Genève/ Zurich/Bâle 2014, 108.

12 ATF 130 III 28 cons. 4.2 ; TF 6B_615/2014 du 2.12.2014 cons. 3 et 4 ; sur toutes ces questions, cf. *David Raedler,* Les enquêtes internes dans un contexte suisse et américain, Lausanne 2018, 504 ss et 526 s.

13 Pour une analyse de cette disposition, cf. *Estelle Mathis-Zwygart,* La surveillance des travailleurs sous l'angle des articles 328b CO et 26

Troisièmement, et c'est l'aspect le plus important en pratique, la surveillance devra respecter la législation applicable en matière de *protection des données.* L'art. 328*b* CO prévoit ainsi que l'employeur ne peut traiter des données concernant le travailleur que dans la mesure où elles portent sur les aptitudes de celui-ci à remplir son emploi ou sont nécessaires à l'exécution du contrat de travail[14]. L'art. 328*b* CO *in fine* renvoie « [e]n outre » aux dispositions de la LPD, laquelle prévoit que tout traitement de données personnelles qui porte atteinte à l'un des principes généraux prévus par cette loi est présumé constituer une atteinte illicite à la personnalité (art. 12 al. 1 et 2 let. a LPD). Les principes susceptibles d'être touchés lors d'une mesure de surveillance sont notamment ceux de reconnaissabilité[15], de proportionnalité, de bonne foi et de finalité[16] (tous listés à l'art. 4 LPD).

À l'instar de ce qui prévaut pour la protection de la personnalité (art. 28 CC), la présomption d'illicéité de l'atteinte peut être renversée en présence d'un motif justificatif tel que le consentement de la victime, un intérêt privé ou public prépondérant, ou encore l'existence d'une base légale (art. 13 al. 1 LPD).

À cet égard, la portée du renvoi de l'art. 328*b* CO à la LPD est débattue en doctrine : certains estiment que si l'employeur se livre à une surveillance en dehors des limites posées par l'art. 328*b* CO, par exemple s'il surveille la messagerie privée d'un employé, celle-ci sera forcément illicite[17]. Un autre courant, plus libéral, soutient au contraire que cette surveillance constitue une simple atteinte aux droits de la personnalité de l'employé, laquelle peut néanmoins être licite s'il existe un motif justificatif au sens de l'art. 13 LPD[18]. Nous adhérons à cette seconde approche, sous réserve du consentement de l'employé, qui ne peut constituer un motif justificatif selon l'art. 13 LPD en raison du caractère (semi-)impératif de l'art. 328*b* CO[19].

B. État des lieux

Ces dernières années, la jurisprudence cantonale, fédérale et européenne a été amenée à trancher de nombreux cas de surveillance d'employés : vidéosurveillance[20], localisation par balise GPS[21], contrôle de l'utilisation d'Internet au travail ou du téléphone portable professionnel[22], voire même utilisation de logiciels-espions[23].

OLT 3, in : Jean-Philippe Dunand/Pascal Mahon (éds), La protection des données dans les relations de travail, Genève/Zurich/Bâle 2017, 312 ss ; cf. ég. ATF 139 II 7 dans lequel le Tribunal fédéral mentionne des études qui démontrent qu'une surveillance électronique constante déploie des effets négatifs sur la santé et le bien-être des travailleurs et leur cause des situations stressantes (cons. 5.5.3).

14 Concernant l'application personnelle, matérielle et temporelle de cette disposition, cf. *Kurt Pärli,* Datenschutz, in : Wolfgang Portmann/Adrian von Kaenel (éds), Fachhandbuch Arbeitsrecht, Expertenwissen für die Praxis, Genève/Zurich/Bâle 2018, 693 ss N 17.15 ss.

15 Le principe de reconnaissabilité (art. 4 al. 2 LPD) suppose que la collecte de données personnelles, et en particulier les finalités du traitement, soient reconnaissables pour la personne concernée.

16 Selon le principe de finalité (art. 4 al. 3 LPD), les données personnelles ne doivent être traitées que dans le but qui est indiqué lors de leur collecte, qui est prévu par une loi ou qui ressort des circonstances. L'utilisation de données récoltées dans un autre but que celui qui était prévu initialement viole ainsi le principe d'immutabilité du but (*Philippe Meier,* Protection des données, Berne 2011, N 725).

17 Préposé fédéral à la protection des données et à la transparence (PFPDT), Guide pour le traitement des données personnelles dans le secteur du travail (personnes privées), 10.2014, 6 ; *Ullin Streiff/Adrian von Kaenel/Roger Rudolph,* Art. 328*b* OR, in : Arbeitsvertrag, Praxiskommentar zu Art. 319-362 OR, 7e éd., Genève/Zurich/Bâle 2012, Art. 328*b* N 3 ; *Christian Flueckiger,* Principes généraux de la protection des données et communications transfrontières dans le cadre des relations de travail, in : Jean-Philippe Dunand/Pascal Mahon (n. 13), La protection des données dans les relations de travail, Genève/Zurich/Bâle 2017, 9 ; *Michel Pellascio,* Art. 328*b* OR, in : Jolanta Kren Kostkiewicz/Stephan Wolf/Marc Amstutz/Roland Fankhauser (éds), OR Kommentar, Schweizerisches Obligationenrecht, 3e éd., Zürich 2016, Art. 328b N 9 ; *Markus Hugentobler,* Datenschutzfalle Assessment Center, PJA 2009 153, 154.

18 *Métille* (n. 11) 106 ; *Manfred Rehbinder/Jean-Fritz Stöckli,* Art. 328b OR, in : Berner Kommentar, Das Obligationenrecht, Berne 2010, Art. 328b N 11 ; *Isabelle Wildhaber/Silvio Hänsenberger,* Internet am Arbeitsplatz, RJB 2016 307, 318 ; *Meier* (n. 16) N 2037 ; *Adrian Staehelin,* Zürcher Kommentar, Der Arbeitsvertrag, Art. 319-330a OR, 4e éd., Genève/Zurich/Bâle 2006, Art. 328b N 12 ; *David Rosenthal,* Art. 328b OR, in : Handkommentar zum Datenschutzgesetz, sowie weitere, ausgewählte Bestimmungen, Genève/Zurich/Bâle 2008, Art. 328*b* N 4 ; *Peter Hafner,* Auswertung der E-Mails von Arbeitnehmern, PJA 2018 1327, 1330.

19 Cf. art. 362 CP. Dans ce sens ég., *Gabriel Kasper/Isabelle Wildhaber,* Big Data am Arbeitsplatz, Datenschutz- und arbeitsrechtliche Herausforderungen von People Analytics in Schweizer Unternehmen, in : Ueli Kieser/Kurt Pärli/Ursula Uttinger (éds) : Datenschutztagung 2018 – Ein Blick auf aktuelle Rechtsentwicklungen, Zurich/Saint-Gall 2019, 198.

20 TF, 6B_536/2009, 12.11.2009 ; 9C_785/2010, 10.6.2011 ; CourEDH, Köpke c. Allemagne, 5.10.2010, no 420/07 ; CourEDH López Ribalda (n. 2).

21 ATF 130 II 425.

22 Utilisation d'Internet à des fins privées : CourEDH (Grande Chambre), *Bărbulescu* c. *Roumanie,* 5.9.2017, no 61 496/08 ; contrôle des sites Internet (soupçon de contenu pornographique) : ATF 143 II 443, CJ GE, ATA/329/2013, 28.5.2013 et TC JU, ADM 92/2009, 25.2.2013 ; contrôle des messages *WhatsApp* échangés sur le portable professionnel : OGer ZH, LA180031-O/U, 20.3.2019.

23 ATF 139 II 7.

1. La proportionnalité comme critère décisif

À la lecture de ces arrêts, on remarque que le critère décisif pour juger de la licéité d'une mesure de surveillance est le respect du *principe de proportionnalité*: la mesure doit être apte à atteindre le but poursuivi (règle de l'aptitude), il ne doit pas exister d'autres mesures moins incisives susceptibles d'atteindre le même but (règle de la nécessité) et une pesée des intérêts fait que l'intérêt à la surveillance l'emporte sur ceux des employés concernés (règle de la proportionnalité au sens étroit). Ce principe doit en effet toujours être respecté, qu'on examine la situation sous l'angle de l'art. 26 OLT 3, de l'art. 328*b* CO ou de la LPD[24]. Dans ce dernier cas, la règle de la proportionnalité au sens étroit correspond d'ailleurs à la pesée des intérêts prévue à l'art. 13 al. 1 LPD et peut donc constituer un motif justificatif à une atteinte qui violerait l'art. 328*b* CO ou les principes généraux de l'art. 4 LPD[25]. La jurisprudence de la CourEDH confirme également que le facteur déterminant est bel et bien celui de la proportionnalité[26].

Concernant la règle de *l'aptitude,* la mesure de surveillance doit permettre à l'employeur de découvrir l'auteur de l'infraction présumée, respectivement d'étayer des soupçons pesant déjà à l'encontre d'un ou plusieurs employés. Il est ainsi nécessaire qu'il existe des soupçons préalables, lesquels doivent être suffisamment concrets et concerner une infraction susceptible de porter atteinte au lien de confiance entre employeur et employé[27].

La deuxième condition, soit la *nécessité,* impose à l'employeur de mettre en place les mesures de surveillance les moins incisives possible. Ainsi, un système de vidéosurveillance ne devrait filmer que ce qui est strictement nécessaire à la découverte de l'infraction, et privilégier une surveillance en différé plutôt qu'en temps réel. Une surveillance informatique ne devrait être envisagée que si d'autres mesures moins invasives – telles que le blocage de certains sites Internet ou d'applications à pure fin privée sur des téléphones de fonction[28] – se sont révélées inefficaces. De plus, l'employeur devrait premièrement procéder à une analyse anonyme des données informatiques, ce qui lui permettra de concrétiser ses soupçons afin de pouvoir procéder, dans un second temps seulement, à une analyse nominale[29]. Dans le même ordre d'idées, il est préférable d'examiner d'abord les seules données secondaires, par exemple relatives aux e-mails envoyés par l'employé, avant d'analyser le contenu en tant que tel.

Enfin, la dernière condition, soit la *proportionnalité au sens étroit,* revient à procéder à une pondération des intérêts entre ceux de l'employé et ceux de l'employeur, afin de déterminer lesquels sont prépondérants. Du côté de l'employé, il s'agit de déterminer l'intensité de l'atteinte à ses droits de la personnalité causée par la surveillance, qui dépend des modalités concrètes de cette dernière ainsi que du caractère privé, voire intime, des données récoltées dans ce cadre. L'intérêt de l'employeur réside dans le fait de découvrir l'auteur de l'infraction présumée, laquelle, si elle est commise à son détriment ou à celui de ses clients, est susceptible de justifier un licenciement immédiat (art. 337 CO)[30]. L'employeur pourra également faire valoir son devoir de protéger la personnalité de ses autres employés (art. 328 CO), le respect de ses directives internes (art. 321*d* CO), ainsi que son intérêt à éviter d'être lui-même tenu pour civilement (art. 101 CO), voire pé-

[24] ATF 130 II 425 cons. 3.3; TF 9C_785/2010 du 10.6.2011 cons. 6.6; cf. ég. *Raedler* (n. 12) 522; *Aurélien Witzig,* Droit du travail, Genève/Zurich/Bâle 2018, N 1641; *Métille* (n. 11) 116 s.

[25] Cf. Dans ce sens ATF 138 II 346 cons. 9.3; *Lucien Müller,* Private Videoüberwachung in öffentlich zugänglichen Räumen – Datenschutzrechtliche Aspekte, Sécurité & Droit 2012 70.

[26] Bărbulescu (n. 24) § 121: «La Cour est consciente que la situation évolue rapidement dans ce domaine [les mesures de surveillance de la correspondance et des autres communications]. Toutefois, elle estime que la proportionnalité et les garanties procédurales contre l'arbitraire sont des éléments essentiels»; CourEDH, *López Ribalda* (n. 2) § 116.

[27] *Staeger/Meier,* Surveillance vidéo sur le lieu de travail – quelques enseignements tirés de l'Arrêt du TF 9C_785/2010 du 10 juin 2011, jusletter 16.4.2012 (n. 23) N 50; CourEDH, *López Ribalda* (n. 2) § 134; cf. déjà l'art. 6.14 al. 2 du Recueil de directives pratiques du BIT sur la protection des données personnelles des travailleurs, 15.6.1997: «Toute surveillance secrète ne saurait être autorisée que s'il existe des soupçons raisonnablement justifiés d'activités criminelles ou d'autres infractions graves».

[28] ATF 139 II 7 cons. 5.5.4; cf. ég. l'art. 141.1 de la Recommandation CM/Rec(2015)5 du Comité des Ministres aux États membres sur le traitement des données à caractère personnel dans le cadre de l'emploi, 1.4.2015: «[e]n ce qui concerne plus particulièrement l'éventuel traitement de données à caractère personnel relatif aux pages internet ou intranet consultées par l'employé, il conviendrait de préférence d'une part d'adopter des mesures préventives, telles que la configuration de systèmes ou l'utilisation de filtres qui peuvent empêcher certaines opérations»; *Jean-Philippe Dunand,* Internet au travail: droits et obligations de l'employeur et du travailleur, *in* Jean-Philippe Dunand/Pascal Mahon (éds), Internet au travail, Genève/Zurich/Bâle 2014, 70.

[29] ATF 139 II 7 cons. 5.4.4; ATF 143 II 443 cons. 4.4.2; *Dunand* (n. 28) 61; *Meier* (n. 16) N 2210, 713 ss; *David Raedler,* L'instruction de l'enquête interne et les données personnelles: naviguer entre volonté d'instruction et nouvelles limites à l'investigation, RDS 2019 317; PFPDT, Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail (économie privée), 9.2013, 10; *Hafner* (n. 18) 1332.

[30] Ce d'autant plus s'il s'agit d'un cadre, dont le comportement s'apprécie avec une rigueur accrue: ATF 130 III 28 cons. 4.1.

nalement (art. 102 CP) responsable des actes de son employé. À rigueur de l'art. 13 al. 1 LPD, il pourrait même invoquer un intérêt public, soit l'intérêt à la découverte et à la poursuite d'infractions[31].

En définitive, plus ses soupçons seront importants et plus l'infraction en cause lui sera préjudiciable, plus l'employeur sera légitimé à mettre en place une mesure de surveillance incisive[32].

2. L'information préalable à la surveillance

L'existence, ou non, d'une *information préalable* donnée aux employés sur la possible mesure de surveillance ainsi que sa nature devra être prise en compte lors de la pesée des intérêts. En effet, l'atteinte au droit de la personnalité de l'employé sera d'autant plus importante s'il n'a pas été informé de cette possibilité (violation du principe de reconnaissabilité, art. 4 al. 4 LPD). Au contraire, plus l'information préalable sera précise, notamment concernant les conditions, la nature et l'ampleur des mesures, moins l'employé sera atteint dans ses droits de la personnalité[33]. Concrètement, l'employeur devrait informer les employés – par exemple au moyen d'un règlement interne – des possibles raisons d'une surveillance, des méthodes et techniques utilisées, ainsi que des données pouvant être collectées dans ce cadre[34].

L'absence d'information préalable ne rend toutefois pas *ipso iure* toute mesure de surveillance illicite[35]. Le tribunal pourra tout de même considérer comme licite une surveillance d'employés qui n'en ont pas été informés de manière préalable[36], à condition qu'il prenne en considération cette absence d'information lors de la pesée des intérêts en présence[37].

Enfin, si la mesure de surveillance n'avait pas pour but d'élucider une infraction, mais qu'elle a néanmoins permis d'en découvrir une, il s'agira également de procéder à une pesée des intérêts telle que mentionnée ci-dessus[38]. Dans ce cas toutefois, l'information préalable de l'employé devra se voir accorder un poids encore plus important. En effet, si non seulement la surveillance n'avait pas pour but de confirmer l'existence de soupçons d'infraction (violation du principe de finalité), mais qu'en plus l'employé n'en avait pas été informé (violation du principe de reconnaissabilité), les intérêts de l'employeur devront être particulièrement importants pour que le traitement des données de l'employé surveillé demeure licite en application de l'art. 13 LPD.

C. Synthèse

Qu'elle soit effectuée à l'aide d'une caméra, d'un logiciel espion ou encore d'une balise GPS, une surveillance est une atteinte aux droits de la personnalité de l'employé. Afin qu'elle soit licite, la surveillance doit dans tous les cas être proportionnée. L'employeur doit ainsi disposer de soupçons d'autant plus concrets que la mesure de surveillance est incisive. De plus, l'employé devrait en principe avoir été préalablement informé de la possibilité d'une telle surveillance, ainsi que de sa nature. Si l'information préalable fait défaut, la surveil-

[31] Cet intérêt public a été retenu par le Tribunal fédéral en matière de vidéosurveillance dans l'arrêt 9C_785/2010 du 10.6.2011 cons. 6.7.3. La question est toutefois controversée : certains admettent que l'intérêt public peut être pris en compte en cas d'infractions (*Hafner* [n. 18] 1335 ; *Rosenthal* [n. 18] art. 328*b* CO N 68). D'autres soutiennent que l'intérêt public ne joue qu'un rôle secondaire (*Meier* [n. 16] N 1612 ss ; *Rosenthal* [n. 18] art. 13 LPD N 20 ; BSK DSG-*Rampini,* art. 13 LPD N 46), voire refusent tout simplement de le prendre en considération (*Stefan Maeder,* Verwertbarkeit privater Dashcam-Aufzeichnungen im Strafprozess, PJA 2018 155, 165 en relation avec la Dashcam ; OGer BE, SK 2013 275, 1.5.2014, cons. 4, concernant la vidéosurveillance).

[32] Cf. *Métille* (n. 11) 128 ; p.ex. si l'employeur soupçonne l'un de ses employés de voler de petites sommes d'argent, il ne pourra pas procéder à une vidéosurveillance qui surveille en permanence et en direct de nombreux employés. Au contraire, si l'infraction est grave, telle une exploitation d'informations d'initiés (art. 154 LIMF) ou une manipulation de cours (art. 155 LIMF), l'employeur pourra collecter les données informatiques des employés soupçonnés en procédant en premier lieu à une analyse anonyme (cf. *supra* II.B.1.) ; cf. *Hafner* (n. 18) 1334.

[33] Dans le même sens, *Pärli* (n. 19) N 17.60.

[34] Cf. art. 6.14 al. 1 du Recueil de directives pratiques du BIT sur la protection des données personnelles des travailleurs de 1997, cf. ég. le « règlement d'utilisation » proposé par le PFPDT [n. 29] Annexe B) ; cf. ég. PFPDT (n. 17).

[35] Dans l'arrêt *Bărbulescu* (n. 22) § 121, la CourEDH ne fait qu'énumérer les facteurs dont « les autorités nationales devraient tenir compte » et qui comprennent, aux côtés de l'information du travailleur, le respect du principe de finalité et de proportionnalité. Cf. *Raedler* (n. 12) 520 s. ; *David Vasella,* Der Fall Bărbulescu, digma 2017 238, 241. *Contra : Kurt Pärli,* Datenschutz im Arbeitsrecht : Blick auf praktische Fälle, *in:* Ueli Kieser/Kurt Pärli/Urslua Uttinger (éds), Datenschutztagung 2018, Zurich/Saint-Gall 2019, 181 et *Witzig* (n. 24) N 1648, lesquels interprètent l'arrêt *Bărbulescu* comme imposant systématiquement une information préalable.

[36] *Pärli* mentionne expressément le fait qu'il peut être renoncé à l'information préalable lorsque la surveillance a pour but de détecter un comportement fautif d'un employé (*Pärli,* Datenschutz [n. 14] 714 s., N 17.60) ; cf. ég. *Métille* (n. 11) 116. Comp. avec le système prévu en droit public fédéral (art. 57o al. 2 let. b LOGA) : ATF 143 II 443 cons. 5.4.

[37] CourEDH, *López Ribalda* (n. 2) § 131.

[38] Cf. *Meier* (n. 16) N 734 ; d'un autre avis, cf. *Hafner* (n. 18) 1335 s.

lance ne sera licite au sens de l'art. 13 LPD que si l'atteinte aux droits de l'employé est particulièrement faible (p.ex. une vidéosurveillance qui ne filme que les mains des employés sur une très courte durée) ou les intérêts de l'employeur, voire l'intérêt public, particulièrement importants (telle une infraction lui portant gravement atteinte).

III. L'exploitabilité au pénal de la preuve illicite recueillie par un particulier

A. Les éléments théoriques

Dès lors qu'il a constaté le caractère illicite d'une preuve, le tribunal doit ensuite examiner si elle reste néanmoins exploitable, c'est-à-dire s'il va pouvoir l'apprécier pour trancher la cause qu'il doit juger.

Le CPP ne traite pas de l'exploitabilité des preuves recueillies de manière autonome[39] par des privés[40]. Depuis son entrée en vigueur, il est de jurisprudence constante que les preuves recueillies illicitement par des particuliers peuvent malgré tout être prises en considération dans une procédure pénale pour autant (1) qu'elles auraient pu être obtenues légalement par les autorités pénales et, cumulativement, (2) qu'une pesée des intérêts justifie leur exploitation[41]. La doctrine majoritaire prône la même analyse[42].

1. La récolte hypothétique par les autorités

La première question à résoudre est la suivante : est-ce que l'autorité de poursuite pénale aurait pu obtenir la preuve litigieuse par elle-même si elle avait été informée des soupçons pesant contre le prévenu ? Le raisonnement sera nécessairement hypothétique : peu importe que la police ou le ministère public n'aient pas effectivement eu connaissance des faits ayant justifié, aux yeux du particulier, la récolte du moyen de preuve[43].

Dans la perspective de l'autorité, l'atteinte aux droits de la personnalité de l'individu concerné (en général le prévenu) correspondra bien souvent à une atteinte à ses droits fondamentaux, ne pouvant être justifiée que par le prononcé de mesures de contrainte (art. 196 ss CPP)[44]. Il s'agira dès lors d'examiner si la méthode employée par le particulier peut être assimilée à une mesure de contrainte prévue par la loi (cf. art. 197 al. 1 let. a CPP) et, dans l'affirmative, si les conditions spécifiques de cette mesure étaient remplies en l'espèce.

À suivre un arrêt du Tribunal fédéral et une partie de la doctrine, seules importent les conditions pouvant s'apprécier de manière abstraite, sans égard aux circonstances concrètes entourant la récolte de la preuve[45]. Parmi ces dernières, on pense notamment à l'existence de soupçons suffisants (art. 197 al. 1 let. b CPP), à la possibilité d'avoir recours à d'autres mesures moins sévères (règle de la subsidiarité, art. 197 al. 1 let. c CPP), ou encore à l'(hypothétique) autorisation de la mesure par le Tribunal des mesures de contrainte (TMC)[46]. Au rang des circonstances abstraites figure, en lien avec des documents subtilisés, l'existence d'un motif d'exclusion du séquestre (art. 264 CPP) ou, pour des enregistrements

[39] Dès lors qu'un particulier agit non pas par lui-même, mais à l'initiative de l'autorité, les règles prévues aux art. 140 s. CPP s'appliquent pleinement. La doctrine s'inspire à cet égard de l'arrêt CourEDH, *van Vondel c. Pays-Bas,* 25.10.2007, nº 38258/03, § 49, commenté par *Gunhild Godenzi,* FP 2 (2008) 77 ss.

[40] L'avant-projet du DFJP prévoyait encore un article 150 relatif aux preuves recueillies par des particuliers : « [l]es preuves qui ont été obtenues de manière punissable *(sic)* par des particuliers ne peuvent être exploitées dans une procédure pénale que si l'intérêt public ou privé à la recherche de la vérité l'emporte sur les intérêts protégés par les dispositions pénales enfreintes ». Fortement critiquée, cette disposition n'a toutefois pas été reprise dans le projet du Conseil fédéral.

[41] TF 6B_739/2018 du 12.4.2019 cons. 1.3 ; TF 6B_531/2018 du 2.11.2018 cons. 1.1 ; TF 1B_234/2018 du 27.7.2018 cons. 3.1 ; TF 6B_911/2017 du 27.4.2018 cons. 1.1 ; TF 1B_474/2017 du 8.11.2017 cons. 2.2 ; TF 1B_231/2017 du 17.8.2017 cons. 2.1 ; TF 6B_1241/2016, du 17.7.2017 cons. 1.2.2 ; TF 6B_667/2016 du 25.1.2017 cons. 1.2 ; TF 1B_76/2016 du 30.3.2016 cons. 2.2 ; TF 6B_786/2015 du 8.2.2016 cons. 1.2 ; TF 6B_983/2013 du 24.2.2014 cons. 3.2 ; TF B_323/2013 du 3.6.2013 cons. 3.4 ; TF 1B_22/2012 du 11.5.2012 cons. 2.4.4. Ces principes ne sont pas nouveaux : cf. déjà ATF 109 Ia 244 (arrêt Schenk) et TF du 9.11.1978, in : RSJ 1981 130.

[42] Voir les nombreux auteurs cités dans l'arrêt du TF 6B_786/2015 du 8.2.2016 cons. 1.2. Cf. ég. *Beat Schnell/Simone Steffen,* Schweizerisches Strafprozessrecht in der Praxis, Berne 2019, 180 ss ; *Gérard Piquerez/Alain Macaluso,* Procédure pénale suisse, 3e éd., Genève/Zurich/Bâle 2011, N 987. La doctrine minoritaire est plus sceptique s'agissant de la première condition : *Guhl* (n. 5) N 308 ss ; *David Mühlemann,* Fairness und Verwertbarkeit unternehmensinterner Untersuchungen, PJA 2018 468 ss, 476.

[43] TF 6B_983/2013 du 24.2.2014 cons. 3.3.1. *Contra : Ludovic Tirelli,* Le vol de données bancaires, Expert Focus 12/2015 1009 ss, 1012, qui exige – selon nous à tort – une connaissance effective par l'autorité.

[44] ATF 145 IV 42 cons. 3.

[45] TF 6B_786/2015 du 8.2.2016 cons. 1.3.1, avec la référence à *Gunhild Godenzi,* Private Beweisbeschaffung im Strafprozess, Zurich 2008, 315 ss ; cf. ég. le commentaire de cet arrêt par *Linda Schmid* in : FP 2017 2 ss, 4.

[46] *Contra,* sur ce dernier point *: Thomas Hansjakob,* Überwachungsrecht der Schweiz, Zurich/Bâle/Genève 2017, N 387, qui propose que le ministère public soumette les preuves reçues par des privés au TMC pour autorisation, ce qui nous paraît dépasser le cadre de la récolte *hypothétique* par l'autorité. La jurisprudence n'examine d'ailleurs pas (spontanément) la question de l'autorisation du TMC : voir p.ex. TF 6B_911/2017 du 27.4.2018 cons. 1.2.

secrets, la présence de l'infraction dans le catalogue permettant d'instaurer des mesures de surveillance secrètes (art. 269 ss CPP)[47] ainsi que la période maximale de six mois pendant laquelle des données secondaires de télécommunication peuvent être demandées avec effet rétroactif (art. 273 al. 3 CPP).

On notera toutefois que cette *approche abstraite* est loin de faire l'unanimité : dans plusieurs arrêts, le Tribunal fédéral examine l'existence de soupçons suffisants au vu des éléments concrètement à disposition du particulier[48], n'hésitant d'ailleurs pas à considérer la preuve comme inexploitable s'il s'avère qu'elle a été récoltée avant même qu'une quelconque infraction n'ait encore été commise[49].

À notre sens, cette récolte hypothétique ne saurait dépendre de l'ensemble des circonstances concrètes prévalant au moment de la récolte effective par le privé, comme le préconisent pourtant certains auteurs, qui vont jusqu'à exiger qu'on vérifie si le procureur en charge ce jour-là était effectivement joignable et aurait dès lors pu ordonner la mesure à temps[50]. Pour autant, on ne peut ignorer la question de l'existence de soupçons suffisants ou, à tout le moins, préalables, qui permet de sanctionner des comportements s'apparentant à de la *fishing expedition*[51].

Il est en revanche admis que l'utilisation par des privés de méthodes d'administration des preuves prohibées par l'art. 140 CPP, telles que la tromperie[52] ou la torture, rend les moyens de preuve ainsi obtenus absolument inexploitables par l'autorité, puisque cette dernière n'aurait elle-même pas pu les récolter valablement (cf. art. 141 al. 1, 1ère phrase CPP)[53].

2. *La pesée des intérêts*

La seconde condition consiste à mettre en balance, d'une part, l'intérêt (privé) du prévenu à ce que le moyen de preuve soit jugé inexploitable et, d'autre part, l'intérêt (public) de l'État à la manifestation de la vérité[54]. Ce dernier sera d'autant plus décisif que l'infraction en cause est grave[55]. La jurisprudence n'hésite pas à s'inspirer de la notion d'*infractions graves* prévue à l'art. 141 al. 2 CPP[56], qui vise essentiellement les crimes (art. 10 al. 2 CP) et semble exclure les délits (art. 10 al. 3 CP) et les contraventions (art. 103 CP)[57]. La doctrine privilégie à juste titre une analyse plus fine, qui prendrait en compte non pas la seule peine-menace, mais la gravité des faits concrètement reprochés au prévenu, à l'instar de ce qui prévaut pour la défense obligatoire (art. 130 let. b CPP) et d'office (art. 132 al. 2 et 3 CPP)[58]. Certains arrêts vont également dans ce sens, en retenant par exemple l'existence d'une infraction grave en cas d'escroquerie aux assurances sociales sur plusieurs années[59], ou encore en la niant en présence d'une unique infraction contre le patrimoine, sans butin important ni autre circonstance aggravante[60].

À l'opposé, l'intérêt du prévenu sera celui tendant à la sauvegarde de ses droits personnels; il dépendra de l'intensité de l'atteinte causée en amont par la récolte de la preuve illicite[61]. La doctrine propose d'y ajouter l'intérêt (public) au caractère équitable de la procédure ainsi que l'intérêt à ce que les par-

47 *Godenzi* (n. 45) 311 ss et 320 s. ; ATF 117 Ia 341 : séquestre d'aveux écrits, confiés à un avocat puis volés, impossible.

48 TF 6B_739/2018 du 12.4.2019 cons. 1.4 ; TF 6B_911/2017 du 27.4.2018 cons. 1.2.2, lequel examine également la règle de la subsidiarité ; cf. ég. CJ GE, ACPR/687/2018, 21.11.2018 cons. 3.2 ; OGer BE, BK 2011 93, 13.7.2011.

49 TF 1B_22/2012 du 11.5.2012 cons. 2.4.4 ; TF 6B_1310/2015 du 17.1.2017 cons. 6. Cf. ég. TC FR, arrêt 501 2013 108, 1.6.2015, cons. 1e ; OGer BE, BK 2012 62, 18.6.2012, cons. 4.2 *ab initio,* in : CAN 2013 Nr. 44 105 ss et BK 2011 9, 22.3.2011, cons. 2.4, in : CAN 2012 Nr. 36 102 ss.

50 *Roberto Fornito,* Beweisverbote im schweizerischen Strafprozess, Saint-Gall 2000, 265.

51 Cf. 137 I 218 cons. 2.3.2 ; KGer SZ, STK 2017 1, 20.6.2017, cons. 3b.aa, pour la *Dashcam.*

52 Sur cette notion, cf. ATF 144 IV 23. Pour un exemple en matière de relation de travail (faux client destiné à tromper un guichetier suspecté d'abus de confiance), cf. TC FR, 501 2014 39, 27.5.2016.

53 *Wolfgang Wohlers/Linda Bläsi,* Dogmatik und praktische Relevanz der Beweisverwertungsverbote im Strafprozessrecht der Schweiz, recht 2015 158 ss, 162 ; *Maeder* (n. 31) 160 ; cf. déjà ATF 109 Ia 244 cons. 2b (arrêt Schenk).

54 ATF 109 Ia 244 cons. 2b (arrêt Schenk).

55 ATF 130 I 126 cons. 3.2 ; 137 I 272 cons. 4.1.2 ; TF 6B_911/2017 du 27.4.2018 cons. 1.2.3. Certains auteurs soutiennent au contraire que plus l'infraction est grave, plus l'intérêt au respect des règles sur la récolte des preuves est grand : *Arnold F. Rusch,* Little Red Corvette, Big Black Box, PJA 2016 403 ss, 404.

56 TF 6B_1311/2017 du 23.8.2017 cons. 2.3, qui rappelle à juste titre que cette disposition ne peut s'appliquer ici que par analogie ; TF 6B_1188/2018 du 26.7.2019 cons. 2.2, analysé ci-dessous (cf. *infra* IV.B.2).

57 ATF 137 I 218 cons. 2.3.5.2 ; TF 6B_287/2016 du 13.2.2017 cons. 2.4.4. ; TF 6B_908/2018 du 7.10.2019, destiné à la publication, cons. 4.2. Sur les différents avis doctrinaux, cf. Komm. StPO-*Wohlers,* Art. 141 N 21a.

58 *Maeder* (n. 31) 161 et 166 ; cf. ég. *Schmid* (n. 63) 5. Sur ces dispositions : ATF 143 I 164.

59 TF 6B_739/2018 du 12.4.2019 cons. 1.4 *in fine* et les références citées.

60 TF 6B_323/2013 du 3.6.2013 cons. 3.5 ; voir aussi TF 1B_26/2016 du 29.11.2016 cons. 4.3.2 : (délit de) violation du secret de fonction (art. 320 CP), sous une forme qui n'était pas particulièrement grave.

61 ATF 109 Ia 244 cons. 2b (arrêt Schenk) ; *Guhl* (n. 5) 130 ss ; *Wohlers/Bläsi* (n. 53) 162.

ticuliers ne soient pas incités à se faire justice eux-mêmes (« *kein Anreiz zu Selbstjustiz* »)[62].

B. L'application à la surveillance de l'employé

Le Préposé fédéral et le Secrétariat d'État à l'économie semblent tous deux partir de l'idée que la surveillance d'un employé soupçonné d'avoir commis une infraction relève des seules autorités pénales, et que les preuves récoltées dans ce cadre par l'employeur seraient déclarées inexploitables en procédure[63]. La réponse n'est pas aussi affirmative et va dépendre des deux conditions développées ci-dessus.

1. La récolte hypothétique par les autorités

En tant qu'elle revient à traiter ses données personnelles, la surveillance d'un employé correspond, dans la perspective de l'autorité, à une atteinte à la protection de sa sphère privée et, plus spécifiquement, à son droit à l'autodétermination en matière d'informations personnelles (art. 13 al. 2 Cst.)[64]. On l'a vu, elle ne se conçoit qu'au travers d'une mesure de contrainte (cf. *supra* III.A.1).

La question – controversée – de l'existence de soupçons préalables devra alors selon nous être examinée dans tous les cas. À cet égard, le Tribunal fédéral a nié l'existence de tels soupçons lors d'un contrôle à grande échelle des données téléphoniques et de comptes de messagerie électronique de l'ensemble des membres et collaborateurs de l'Université de Zurich, soulignant que le soupçon devait être dirigé contre une ou plusieurs personnes déterminées, à défaut de quoi la mesure ne servait pas à l'étayer, mais bien seulement à le fonder[65].

La question ensuite de la légalité de la mesure que l'autorité aurait – hypothétiquement – pu mettre en œuvre dépendra du type de surveillance : un système secret de *vidéosurveillance* ou d'*enregistrement audio* s'analysera soit comme une autre mesure technique de surveillance (art. 280 s. CPP), soit comme une observation (art. 282 s. CPP), selon le caractère public ou librement accessible des lieux ou conversations concernés (comp. art. 280 let. a et b avec art. 282 al. 1 CPP)[66]. La distinction n'est pas dénuée d'importance : si l'observation est possible tant pour les crimes que les délits (art. 282 al. 1 let. a CPP), les autres mesures techniques de surveillance ne s'envisagent que pour certaines infractions bien précises (principalement des crimes), listées à l'art. 269 al. 2 CPP (auquel renvoie l'art. 281 al. 4 CPP).

L'infrastructure technique à disposition de l'employeur lui permet désormais d'accéder aisément à un nombre important de *données informatiques* concernant ses employés – par exemple les données secondaires de connexion à Internet ou au service interne de messagerie électronique, mais également le contenu des e-mails eux-mêmes, sauvegardés sur un serveur interne –, données que l'autorité pénale aurait théoriquement pu obtenir par le biais d'un séquestre (art. 263 ss CPP) auprès de l'employeur directement[67]. Dans le cas de l'Université de Zurich, le Tribunal fédéral a considéré que les données récoltées étaient couvertes par le secret des télécommunications, ce d'autant plus que l'utilisation de la messagerie électronique à titre privé était admise dans une certaine mesure par le règlement interne de l'université[68]. Sur cette base, il faut retenir que le contrôle, par l'employeur, de données relatives à l'utilisation à des fins privées d'Internet ou du courrier électronique sur le lieu de travail, pour autant qu'une telle utilisation soit tolérée ou expressément autorisée au sein de l'entreprise, s'apparente à une mesure de surveillance de la correspondance par poste et télécommunication (art. 269 ss CPP)[69]. Dès lors que le contrôle concerne le contenu des e-mails eux-mêmes, il s'agira donc de déterminer si l'infraction entre dans la liste prévue à l'art. 269 al. 2 CPP. Si, en revanche, le contrôle porte sur des données secondaires (fichiers journaux des connexions à Internet ou des e-mails envoyés/reçus), la mesure s'analysera sous l'angle de l'art. 273 CPP, qui vise tant les crimes que les délits (et l'art. 179^{septies} CP), mais ne permet pas l'exploitation de données antérieures à six mois (al. 3).

Enfin, l'installation d'un *logiciel-espion* sur l'ordinateur ou le téléphone portable de l'employé équivaut à l'utilisation

[62] BSK StPO-*Gless,* Art. 141 N 42 ; *Maeder* (n. 31) 160 s. et les références citées.

[63] PFPDT, Explications sur la surveillance téléphonique sur le lieu de travail, novembre 2014, ch. 3.3 ; SECO, Commentaire de l'art. 26 OLT 3, 3.2013, ch. 1.

[64] ATF 145 IV 42 cons. 4.2.

[65] TF 1B_26/2016 du 29.11.2016 cons. 4.3.1 (rendu à cinq juges), commenté par *Konrad Jeker,* FP 6 (2017) 388 ss.

[66] Par exemple une pièce exclusivement réservée aux employés (salle du coffre), par rapport à un espace accessible aux clients (rayonnages d'un magasin d'alimentation). Sur la distinction : BSK StPO-*Eugster/Katzenstein,* Art. 280 N 30 ss et 282 N 5.

[67] Cf. l'analogie avec l'ATF 140 IV 181 cons. 2.6, confirmé par l'ATF 143 IV 270 cons. 4.6, pour le séquestre d'e-mails auprès du fournisseur (suisse) du service de messagerie.

[68] TF 1B_26/2016 du 29.11.2016 cons. 4.2.

[69] Plus nuancé : *Hansjakob* (n. 46) N 319 ss, qui raisonne en fonction de la taille de l'entreprise.

d'un programme informatique spécial de surveillance de la correspondance par télécommunication (art. 269ter CP, entré en vigueur le 1er mars 2018), communément appelé GovWare[70]. Un tel procédé, plus invasif qu'une mesure de surveillance «classique», ne sera admissible qu'aux fins de poursuivre des infractions justifiant une investigation secrète (art. 269ter al. 1 let. b CPP, qui renvoie à la liste plus restrictive de l'art. 286 al. 2 CPP).

2. La pesée des intérêts

Telle qu'exposée ci-dessus, la pesée des intérêts devra tenir compte tant de la gravité des faits concrètement reprochés que de l'atteinte aux droits de la personnalité du prévenu, ainsi que, de manière plus générale, du caractère équitable de la procédure pénale. La question sera de savoir s'il existe un *intérêt supérieur* à ce qu'une preuve, récoltée par l'employeur de manière illicite, soit admise au procès pénal contre le prévenu. À ce stade, les *intérêts privés* dont pouvait se prévaloir l'employeur au moment de juger de l'illicéité – contrôler la bonne exécution du travail ou étayer un soupçon d'infraction pénale, justifiant, cas échéant, un licenciement immédiat – ne jouent qu'un rôle secondaire ; tout au plus pourrait-on prendre en compte l'intérêt de l'employeur s'il est lésé (art. 115 CPP) et s'est constitué partie plaignante (art. 118 CPP) dans la procédure menée contre son (ex-)employé.

Certains critères pertinents au stade de l'illicéité déjà (cf. *supra* II.) le sont également pour l'analyse de l'exploitabilité : l'intensité de l'atteinte aux droits de l'employé, si elle plaide pour l'illicéité de la preuve – par exemple une vidéosurveillance permanente, non floutée, débordant du cadre strictement professionnel – devrait également plaider en faveur de son inexploitabilité. À l'inverse, l'intérêt public à la manifestation de la vérité aura déjà pu être pris en compte, dans une certaine mesure[71], au stade de la pesée des intérêts selon l'art. 13 al. 1 LPD, de sorte que s'il n'a pas été décisif à ce stade, il ne pèsera pas lourd dans la balance. Il en résulte que bien souvent, une preuve déclarée illicite sera également jugée inexploitable en procédure. On réservera toutefois les cas où la surveillance met au jour des faits ne présentant aucun rapport avec la relation de travail, appartenant à la sphère strictement privée de l'employé et ne portant pas gravement atteinte à la réputation ou au fonctionnement de l'entreprise[72]. Les preuves ainsi récoltées pourraient, malgré leur caractère illicite, néanmoins être exploitées si elles portent sur une infraction grave.

IV. Deux précédents regrettables

A. L'ATF 143 IV 387 (l'observation de l'assuré)

Dans un arrêt relativement récent, qui avait trait à l'observation d'un assuré par un détective privé, mandaté par une assurance privée[73], la Ière Cour de droit public du Tribunal fédéral a développé un certain nombre de considérations générales sur la récolte de preuves par les particuliers qui sont de nature à remettre en question les principes cohérents développés ci-dessus.

1. Quant à la licéité de la preuve

Premièrement, amené à statuer sur le caractère illicite de l'observation menée par le détective privé, le Tribunal fédéral considère qu'au vu de l'atteinte causée à la sphère privée (art. 13 al. 1 Cst.) de l'assuré, cette observation équivaut à une observation par les autorités pénales (art. 282 s. CPP), et donc à une mesure de contrainte (au sens de l'art. 196 let. a CPP)[74]. Or, de telles mesures ne peuvent être ordonnées que par le ministère public, les tribunaux et, dans les cas prévus par la loi, la police. Les rares cas dans lesquels des particuliers peuvent exceptionnellement appliquer des mesures de contrainte et porter atteinte aux droits fondamentaux des individus sont expressément réglementés par le CPP (cf. art. 218 et 263 al. 3 CPP) et, toujours selon notre Haute Cour, l'observation n'en fait pas partie. Cette mesure est par conséquent illicite[75].

Le raisonnement ne convainc pas. Au-delà de l'application des droits fondamentaux à une observation ordonnée par une assurance (de responsabilité civile) privée[76], c'est surtout le rapprochement avec les mesures de contrainte (art. 196 ss CPP) qui nous paraît problématique. Ces mesures sont en ef-

[70] GovWare provient de *Government Software ;* sur cette notion et la novelle en général, cf. Message du Conseil fédéral du 27.2.2013 concernant la loi fédérale sur la surveillance de la correspondance par poste et télécommunication, FF 2013 2379 ss.

[71] Cf. *supra* (n. 31) sur le caractère controversé de cet intérêt public.

[72] De tels faits ne seraient d'ailleurs pas suffisants pour justifier un licenciement immédiat pour justes motifs (art. 337 CO) de l'employé, et cela même, selon le Tribunal fédéral, s'ils sont constitutifs d'actes d'ordre sexuels avec des enfants : TF 4C.431/2005 du 31.1.2006.

[73] Pour une analyse critique de cet arrêt, cf. *Hirsch* (n. 9).

[74] ATF 143 IV 387 cons. 4.2.

[75] ATF 143 IV 387 cons. 4.2.

[76] Sur cette question : *Thomas Gächter/Michael E. Meier,* Observation – ein Rechtsinstitut unter Beobachtung, Jusletter 11.12.2017, N 68 et 95 ; *Hirsch* (n. 9) N 59 ss et 88 ; ATF 136 III 410 cons. 2.1 ; TF 6B_1241/2016 du 17.7.2017 cons. 1.2.1.

fet l'apanage des autorités de poursuite pénale ; elles ne sauraient en aucun cas constituer une grille de lecture pour juger de la licéité des preuves récoltées par les particuliers, question qui doit être tranchée à l'aune du seul droit privé ou pénal applicable[77].

La Cour de droit pénal du Tribunal fédéral ne dit elle-même pas autre chose lorsqu'elle souligne que le CPP ne règle que le recueil des preuves par les autorités pénales, la maxime de l'instruction (art. 6 al. 1 CPP) ne créant aucun monopole de l'État à cet égard ; les parties et autres participants à la procédure demeurent libres de mener leurs propres enquêtes et d'apporter des preuves à charge ou à décharge au procès[78].

Transposé au cas de la surveillance de l'employé, l'ATF 143 IV 387 aurait pour fâcheuse conséquence que toute vidéosurveillance ou analyse de données informatiques serait considérée *ipso iure* comme illicite, pour la seule raison qu'elle reviendrait à une mesure de contrainte non prévue par le CPP. Si, on l'a vu, cette question peut jouer un rôle au stade de l'exploitabilité de la preuve (notamment en lien avec la récolte hypothétique par l'autorité), elle est toutefois dénuée de pertinence au moment de juger de son illicéité.

2. Quant à l'exploitabilité de la preuve

Après avoir retenu que la preuve est illicite, le Tribunal fédéral examine la question du caractère exploitable de celle-ci. Comme l'affaire ne concernait pas un jugement au fond, mais une levée de scellés, seule une inexploitabilité manifeste pouvait entrer en ligne de compte[79]. Le Tribunal fédéral se demande si l'observation litigieuse constitue une preuve absolument inexploitable au sens de l'art. 141 al. 1 CPP, soit une preuve administrée en violation de l'art. 140 CPP ou lorsqu'une autre disposition du CPP dispose expressément qu'elle n'est pas exploitable. Le Tribunal fédéral cite à titre d'exemple des écoutes téléphoniques privées illégales, non autorisées par un juge, l'utilisation de dispositifs techniques de surveillance par des privés ou encore une investigation secrète menée par un détective privé (art. 277, 281 al. 4 et art. 289 al. 6 CPP)[80]. En l'occurrence, la loi ne prévoit pas que le résultat d'observations privées ou d'autres mesures probatoires non soumises à l'autorisation d'un juge (telles que des expertises privées) est inexploitable, de sorte que l'on ne se trouve pas face à une preuve absolument inexploitable au sens de l'art. 141 al. 1 CPP[81]. Le Tribunal fédéral procède enfin à une pesée des intérêts au sens de l'art. 141 al. 2 CPP, pour arriver à la conclusion que la preuve litigieuse n'était pas manifestement inexploitable[82].

Cette approche est, ici aussi, critiquable, en tant qu'elle applique directement – et sans justification aucune – l'art. 141 CPP à la récolte de preuves par des personnes privées[83]. Ensuite, elle s'affranchit purement et simplement de la condition de la récolte hypothétique par les autorités, qui repose sur une jurisprudence désormais établie, et revient au contraire à exiger une intervention concrète de l'autorité, par l'entremise du Tribunal des mesures de contrainte (TMC). En effet, à suivre les bases légales citées à l'appui du raisonnement du Tribunal fédéral (art. 277, 281 al. 4 et art. 289 al. 6 CPP), une preuve récoltée grâce à une mesure de surveillance secrète (notamment une écoute téléphonique ou un autre dispositif technique) serait inexploitable pour la seule et unique raison que cette mesure n'a pas été avalisée par le TMC. Or, c'est bien le propre de toute preuve récoltée par un privé de ne pas avoir été autorisée, en amont, par une quel-

[77] Cf. dans ce sens TF 6B_536/2009 du 12.11.2009 cons. 3.3.1, qui exclut d'examiner les conditions des mesures de contrainte au stade de la licéité ; *Yvan Jeanneret/André Kuhn,* Précis de procédure pénale, 2e éd., Berne 2018, N 14089 et n. 330.

[78] TF 6B_786/2015 du 8.2.2016 cons. 1.2 ; TF 6B_323/2013 du 3.6.2013 cons. 3.3. Dans le même sens, cf. *Maeder* (n. 31) 156 s.

[79] ATF 143 IV 387 cons. 4.4, confirmé pour l'autorité de recours (art. 393 ss CPP) par l'ATF 143 IV 475 cons. 2.7, ce qui permet d'affirmer que la question de l'exploitabilité des preuves récoltées par des privés devrait en principe être réservée au juge du fond, compte tenu de la pesée des intérêts qu'elle comporte (cf. *supra* III.A.2). Cf. dans ce sens OGer BE, BK 2019 100, 23.5.2019.

[80] ATF 143 IV 387 cons. 4.5 : « *Zu den Beweismitteln, welche die StPO als unverwertbar bezeichnet* (Art. 141 Abs. 1 Satz 2 StPO) *und die deshalb ‹in keinem Fall verwertbar› sind (sogenanntes ‹absolutes› Verwertbarkeitshindernis), gehören insbesondere nicht richterlich genehmigte, illegale private Telefonabhörungen, der Einsatz technischer Überwachungsgeräte durch Private oder die verdeckte Ermittlung durch Privatdetektive* ».

[81] ATF 143 IV 387 cons. 4.5.

[82] ATF 143 IV 387 cons. 4.6.

[83] *Fabian Teichmann/Marco Weiss,* Observationen durch Privatdetektive – Bemerkungen zu BGE 143 IV 387, Revue de l'avocat 2018 441 ss, 444 considèrent qu'avec sa constitution de partie plaignante, les actions de l'assurance privée devaient être directement imputées à l'État et donc soumises à l'art. 141 CPP. Cette opinion ne peut être suivie : ce qui est déterminant, c'est de savoir si le privé – qu'il soit partie plaignante ou lésé, voire même simple tiers – a agi de manière autonome par rapport aux autorités pénales (cf. n. 39). Or, en l'espèce, l'observation litigieuse avait eu lieu à l'initiative de l'assurance et bien avant l'ouverture de la procédure pénale, ce qui permet de nier une quelconque implication des autorités étatiques et, partant, l'application des règles en matière de récoltes de preuves auxquelles elles sont soumises. Cf. ég. *Gächter/Meier* (n. 76) N 68.

conque autorité ; une telle autorisation lui enlèverait d'ailleurs tout caractère « privé ». Enfin, soumettre les preuves issues de mesures de surveillance privées à l'art. 141 CPP revient à éluder la condition de la pesée des intérêts, puisqu'en l'absence d'autorisation du TMC, la sanction sera une inexploitabilité absolue et non relative des moyens de preuve récoltés (art. 141 al. 1, 2e phrase CPP).

En définitive, outre qu'elle n'est pas confortée par les références citées dans l'arrêt[84], la solution du Tribunal fédéral vient conditionner l'exploitabilité des preuves récoltées par les particuliers à une exigence qui ne doit précisément pas s'appliquer à ceux-ci, car s'adressant, une fois de plus, exclusivement aux autorités de poursuite pénale. Il y a lieu de s'en tenir à la formule consacrée : (1) examen de la récolte hypothétique par les autorités – sans qu'une autorisation effective du TMC ne soit nécessaire – puis (2) pesée des intérêts – lors de laquelle l'art. 141 al. 2 CPP s'appliquera tout au plus par analogie, et non directement comme dans l'ATF précité[85].

B. L'arrêt du Tribunal fédéral sur la Dashcam (6B_1188/2018*)

Dans un second arrêt encore plus récent, destiné à la publication au Recueil officiel et annoncé par voie de communiqué de presse, la Cour de droit pénal du Tribunal fédéral est venue mettre un terme au vif débat qui portait depuis quelques années déjà sur l'exploitabilité au procès pénal d'enregistrements recueillis par un automobiliste au moyen d'une caméra embarquée (*Dashcam*)[86]. La portée de ce très court arrêt (six pages) dépasse toutefois cette seule problématique, puisque c'est en réalité l'entier du système des preuves récoltées par des privés qui est, une nouvelle fois, remis en question.

1. Quant à la licéité de la preuve

Le Tribunal fédéral relève que l'enregistrement vidéo d'un autre automobiliste par une *Dashcam* est un traitement de données personnelles qui ne respecte pas le principe de reconnaissabilité (art. 4 al. 4 LPD)[87]. Il s'agit donc d'une atteinte à la personnalité au sens de l'art. 12 LPD, laquelle est illicite à moins d'être justifiée par un motif prévu à l'art. 13 LPD (cf. *supra* II.A). Suivant l'approche défendue par *Guhl*[88], notre Haute Cour s'éloigne toutefois de cette conception classique de l'illicéité et lui donne une *définition autonome* en droit procédural : un moyen de preuve récolté par un privé sera qualifié d'illicite aussitôt qu'il contrevient à une disposition matérielle du droit suisse (en l'occurrence l'art. 4 al. 4 LPD), et ce peu importe qu'un motif justificatif – tel qu'un intérêt privé ou public prépondérant (art. 28 al. 2 CC et art. 13 al. 1 LPD) – puisse, en droit privé, lever le caractère illicite de l'atteinte[89]. Pour le Tribunal fédéral, la pesée des intérêts selon l'art. 13 al. 1 LPD oppose les intérêts de la personne qui traite les données à ceux de la personne concernée, alors que la question de l'exploitabilité d'une preuve au pénal dépend du droit de répression *(Strafanspruch)* de l'État et du droit du prévenu à une procédure équitable ; les intérêts du particulier ayant traité les données doivent s'effacer dans ce cadre[90].

Bien que l'on puisse comprendre les motifs à la base de l'arrêt – éviter que dans une procédure pénale, une preuve soit déclarée licite, et donc nécessairement exploitable, en raison des seuls intérêts privés prépondérants de celui qui l'a récoltée – cette nouvelle définition de l'illicéité en droit procédural nous paraît toutefois difficilement justifiable[91].

D'un point de vue dogmatique d'abord, on peine à comprendre comment une preuve, pourtant récoltée dans le respect de l'ordre juridique, peut être considérée comme illicite du seul fait qu'elle est ensuite produite dans une procédure pénale. La doctrine quasi unanime prône d'ailleurs une approche uniforme de la notion d'illicéité et examine la présence d'un motif justificatif dans un contexte de droit procé-

[84] Les arrêts cités (ATF 143 IV 270 ; 141 IV 284 et 141 IV 289) ne concernent pas les privés. La doctrine citée mentionne soit l'approche classique du Tribunal fédéral et les deux conditions cumulatives (cf. StPO Komm.-*Hansjakob,* Art. 277 N 11-12, Art. 282 N 36), soit ne se prononce tout simplement pas sur la question (BSK StPO-*Jean-Richard-dit-Bressel,* Art. 277 N 3-5).

[85] Critiques également quant à l'analyse du Tribunal fédéral à l'aune des art. 140 s. CPP : *Jeanneret/Kuhn* (n. 77) N 9011, n. 69.

[86] TF 6B_1188/2018 du 26.9.2019.

[87] TF 6B_1188/2018 du 26.9.2019 cons. 3.1 et 3.2.

[88] *Guhl* (n. 5) N 252 ss.

[89] TF 6B_1188/2018 du 26.9.2019 cons. 3.3 et 4.

[90] TF 6B_1188/2018 du 26.9.2019 cons. 3.3, étant précisé que *Guhl* (n. 5) N 253 propose pour sa part de prendre en compte ces motifs justificatifs dans le cadre de la pesée des intérêts au stade de l'exploitabilité.

[91] Cf. ég. critique *David Vasella,* 6B_1188/2018 : Verwertbarkeit privater Dashcam-Aufnahmen im Strafprozess hier verneint, in : datenrecht.ch, 13.10.2019 (<https://datenrecht.ch/6b_1188-2018-verwertbarkeit-privater-dashcam-aufnahmen-im-strafprozess-hier-verneint/>) consulté le 23.10.2019.

dural également[92]. Le Tribunal fédéral lui-même en a déjà fait de même dans un passé proche[93].

Cette définition autonome de l'illicéité est par ailleurs source d'une importante insécurité juridique : comment appréhender le principe de proportionnalité, érigé en principe général de la LPD (art. 4 al. 2 LPD) et donc constitutif d'une norme matérielle du droit suisse au sens de cette nouvelle jurisprudence, mais dont l'examen suppose une pesée des intérêts (règle de la proportionnalité au sens étroit), étape que le Tribunal fédéral voudrait précisément éviter lors de l'examen de la licéité ? D'autres éléments que les motifs justificatifs devraient-ils également être ignorés, par exemple les actes licites en droit pénal (art. 14 ss CP) ? Le consentement est-il considéré comme un motif justificatif ou lève-t-il tout de même l'illicéité d'une atteinte au sens du droit procédural[94] ? Cette nouvelle notion d'illicéité est-elle transposable en procédure civile et administrative[95] ?

D'un point de vue plus pratique enfin, la nouvelle approche du Tribunal fédéral devrait entraîner une augmentation drastique des cas de preuves illicites : dans le contexte qui nous occupe, bien rares seront les situations où une mesure de surveillance mise en place par l'employeur ne touchera à aucun principe général de la protection des données. De manière plus générale, toute photographie ou vidéo d'autrui, obtenue sans son consentement, sera désormais considérée comme illicite au regard du droit de procédure, car constitutive d'une atteinte au droit à l'image (et donc à la personnalité)[96] de l'individu concerné, sans qu'une quelconque pesée des intérêts puisse avoir lieu. Ce constat pourrait d'ailleurs aboutir à des situations clairement insatisfaisantes si on y rajoute les développements du Tribunal fédéral relatifs cette fois-ci à l'exploitabilité de la preuve.

2. Quant à l'exploitabilité de la preuve

Dans ce même arrêt, le Tribunal fédéral décide d'appliquer directement le critère d'« infractions graves » prévu à l'art. 141 al. 2 CPP au régime des preuves récoltées par des privés, précisant que du point de vue du prévenu, il est sans importance de savoir qui, de l'autorité ou du particulier, a collecté les preuves auxquelles il est confronté en procédure[97]. En l'espèce, les faits reprochés avaient été qualifiés par l'*Obergericht* zurichois de violations tantôt simples, tantôt graves des règles de la circulation routière (art. 90 al. 1 et 2 LCR), soit des infractions de degré contraventionnel et délictuel, ce qui ne suffit pas pour les qualifier de graves au sens de l'art. 141 al. 2 CPP et conduit à l'inexploitabilité des preuves récoltées au moyen de la *Dashcam,* sans que la (délicate) question de la récolte hypothétique par les autorités ne doive être tranchée[98].

Cette approche nous paraît trop rigide, en ce qu'elle revient à ne permettre de pesée des intérêts qu'en présence d'infractions graves, soit en définitive des crimes (art. 10 al. 2 CP), et donc à qualifier automatiquement[99] d'inexploitable toute preuve utile à la poursuite d'une infraction de degré moindre. Or, s'il ne fait pas de doute que l'intérêt de l'État à l'exploitabilité de la preuve sera d'autant plus important que l'infraction en cause est grave (cf. *supra* III.A.2), on ne voit pas que cette pesée des intérêts puisse être réservée aux seuls crimes, à l'exclusion de délits tels que la gestion déloyale (art. 158 CP) ou la corruption privée (art. 322^{octies} s. CP). Par ailleurs, le Tribunal fédéral paraît se fonder sur la seule distinction crime/délit, qui dépend du critère abstrait de la peine-menace des infractions en cause, alors que c'est bien plus la gravité des faits concrètement reprochés qui doit être

92 Cf. les nombreux auteurs cités par *Guhl* (n. 5) N 252 nbp 564, ainsi que les auteurs s'étant précisément prononcés sur la problématique de la *Dashcam : Maeder* (n. 31) 164 ss ; *Markus Mohler,* Zur Frage der Gerichtsverwertbarkeit von Dashcam-Aufnahmen im Strassenverkehr, Sicherheit & Recht 1/2019 32 ss, 38 ; *Dominique Arnosti,* Dashcam : Risiko oder Garant im (Rechts)Verkehr ?, Genève/Zurich/Bâle 2019, N 103 ss ; *Matthias Maager,* Verwertbarkeit privater Dashcam-Aufzeichnungen im Strafverfahren, sui generis 2018, N 7 ss et 39 ss ; *Lorenz Gmünder/Christoph Reut/Stefan Zuber,* Zur Verwertbarkeit von privaten Dashcam-Aufnahmen im Zivilprozess, Strassenverkehr 3/2018 54 ss, 59 ; cf. ég. les auteurs cités dans l'arrêt 6B_1188/2018 cons. 4 et KG Schwyz, STK 2017 1, 20.6.2018, cons. 3b.

93 TF 6B_1310/2015 du 17.1.2017 cons. 5.4 et 5.5, sous l'angle de l'art. 28 CC ; cf. déjà TF 6B_536/2009 du 12.11.2009 cons. 3.7.

94 *Guhl* considère singulièrement que le consentement n'est pas réellement un motif justificatif, mais lève néanmoins le caractère illicite d'une atteinte au sens du droit procédural (*Guhl* [n. 5] N 267). Nous rejoignons ce raisonnement dans son résultat, sous la réserve toutefois du consentement donné par l'employé, lequel est sujet à caution en raison du rapport de subordination avec l'employeur.

95 En procédure civile, cf. *Yves Rüedi,* Materiell rechtswidrig beschaffte Beweismittel im Zivilprozess, Zurich/Saint-Gall 2009, N 352 ss.

96 Cf. ATF 138 II 346 cons. 8 (arrêt Google Street View).

97 TF 6B_1188/2018 du 26.9.2019 cons. 2.2. Le Tribunal fédéral se réfère également à l'art. 150 de l'avant-projet du CPP (cf. n. 40), lequel ne prévoyait qu'une simple pesée des intérêts, indépendamment de la gravité de l'infraction en cause, point qui avait été critiqué lors de la procédure de consultation.

98 TF 6B_1188/2018 du 26.9.2019 cons. 4.

99 Si le Tribunal fédéral parle certes de *« Interessenabwägung zuungunsten der Verwertung »* (cons. 4), il ne procède en l'espèce à aucune véritable pesée des intérêts et se fonde uniquement sur les infractions en cause.

déterminante[100] : ainsi, un vol isolé dans la caisse de l'employeur, bien que qualifié de crime (art. 139 CP), devrait peser moins lourd que la révélation d'un secret commercial essentiel à une entreprise concurrente, constitutive d'un simple délit (art. 162 CP).

Cumulé avec la nouvelle définition autonome de l'illicéité en droit de procédure, le raisonnement du Tribunal fédéral revient en définitive à qualifier de totalement inexploitable une photographie ou une vidéo prise par un particulier afin de prouver l'existence d'une injure, d'une menace, de lésions corporelles simples ou d'une rixe, puisqu'il ne s'agit pas d'infractions graves. Cette situation n'est pas sans conséquence pour les avocats : selon une jurisprudence récente, l'avocat ne peut, sous l'angle du devoir de diligence (art. 12 let. a LLCA), produire en procédure une preuve illicite que s'il a de bonnes raisons de penser qu'elle sera tout de même exploitable[101]. Or, en raison de ce nouvel arrêt, l'avocat diligent devra bien trop souvent renoncer à des moyens de preuve qui, d'une part, seront très rapidement qualifiés d'illicites et, d'autre part, ne pourront être exploités que si les infractions en cause sont des crimes.

V. Conclusion

La question posée en introduction était de savoir si l'employeur qui nourrit des soupçons envers l'un de ses employés peut, plutôt que de faire appel aux autorités de poursuite pénale, mettre en place lui-même une mesure de surveillance puis, si le résultat de celle-ci s'avère probant, produire en procédure les moyens de preuve ainsi obtenus.

Cette question a été l'occasion de revenir sur le régime applicable aux preuves récoltées par des particuliers, qui nécessite premièrement d'examiner le *caractère licite* des moyens de preuve. Qu'il procède à une vidéosurveillance ou à une surveillance informatique, l'employeur est tenu de respecter la législation en matière de protection des données. Il devrait ainsi récolter les données uniquement pour prouver l'infraction en question (principe de finalité) et informer préalablement ses employés de la possibilité d'une telle surveillance (principe de reconnaissabilité). En pratique, c'est avant tout sous l'angle du principe de proportionnalité que s'examinera la question de la licéité de la mesure de surveillance. Dans ce cadre, l'atteinte à la personnalité de l'employé concerné pourra être justifiée par l'intérêt prépondérant de l'employeur, ce qui lève à notre sens tout caractère illicite et permet au juge d'exploiter les moyens de preuve sans autre espèce de restriction.

Si toutefois la preuve devait être qualifiée d'illicite, son *exploitabilité* par le juge pénal dépendra de la double condition de sa récolte hypothétique par les autorités et d'une nouvelle pesée des intérêts, qui dépendra cette fois-ci essentiellement de l'intérêt à la manifestation de la vérité et devra tenir compte tant de la gravité (concrète) des faits reprochés à l'employé que de l'intensité de l'atteinte à sa personnalité.

Ce raisonnement en deux étapes – licéité, puis exploitabilité – ne va pas forcément de soi et trouve parfois ses limites dans la diversité des situations pouvant se présenter et les nombreux éléments à prendre en compte à chaque stade. Il apporte pourtant cohérence et sécurité juridique au régime des preuves récoltées par les privés. Certains arrêts récents du Tribunal fédéral viennent désormais le remettre en question, en proposant d'appliquer directement aux particuliers des règles strictes, pensées pour les autorités pénales (ATF 143 IV 387), ou en retenant une notion autonome de l'illicéité en procédure (6B_1188/2018*), avec pour conséquence qu'un nombre toujours plus grand de moyens de preuve sera frappé d'inexploitabilité. En filigrane, on peut y lire la volonté de limiter la marge de manœuvre laissée aux particuliers dans la récolte autonome de preuves. Ce dernier phénomène est pourtant une réalité, notamment dans les relations de travail ; bien souvent les employeurs préfèrent étayer à l'interne les soupçons d'infractions pénales pesant contre leurs employés plutôt que de saisir directement – et parfois à tort – les autorités pénales. Il s'agit de s'en rappeler et d'appliquer strictement une méthode certes complexe, mais qui garantit le juste équilibre entre autonomie des parties et équité de la procédure pénale.

[100] Cf. *supra* III.A.2. À cet égard, l'arrêt cité à l'appui du raisonnement du Tribunal fédéral (ATF 137 I 218) examinait bien le comportement concrètement reproché (cons. 2.3.5.2) lequel était – même pour un simple délit – ensuite mis en balance avec l'intérêt du prévenu (cons. 2.3.5.3 et 2.3.5.4), étapes qui sont ici simplement ignorées.

[101] ATF 144 II 473 cons. 5.1.