特別セミナー講演

防犯カメラの高機能化と法的規制の新たな動向

首都大学東京・都市教養学部法学系教授　星　周一郎

街頭設置カメラについては、その画質の向上をはじめとする機能の高度化に伴い、その法的な設置根拠や許容限界についても、新たな観点から議論をする必要が生じています。

1.映像等情報の個人情報該当性

従来のアナログ技術で人物を撮影したカメラ映像は、「個人を容易に識別できないので個人情報にはあたらないが、警察での捜査の過程での他の情報との突合により、個人情報にあたる可能性があるもの」という、ややあいまいな位置づけだったといえます。

これに対し、高精細・高画質のデジタル画像では、画角等にもよりますが、それ自体で、個人を識別できる映像となる場合が圧倒的に多くなっています。個人情報該当性の判断では、個人の氏名まで識別できる必要はありません。そのため、そういった映像は、個人情報にあたることになります。また、顔認証などに用いる対照データも、個人識別符号として個人情報にあたります（個人情報保護法2条）。

映像や識別符号が個人情報に該当するならば、カメラの設置者が個人情報取扱事業者であれば、個人情報保護法上の、(1)個人情報である段階での諸責務、(2)個人情報データベース等を構成する個人データとされた段階での諸責務、(3)個人データを6か月以上保有する保有個人データに該当する段階での諸責務を、それぞれ遵守する必要が生じます。

2.個人情報とプライバシー

カメラ映像が個人情報にあたるとなると、「えっ!じゃあ、もう使ってはダメなの?」といった反応を示す向きもあるかもしれません。しかし、この認識は誤りです。個人情報保護法は「個人情報利用禁止法」ではありません。2017年9月に表面化した「年金支給漏れ」に象徴されるように、個人情報の適正な利活用は、むしろ有用・必須で、個人に利益をもたらすのであって、個人情報保護法もそれを推奨しています（個人情報保護法1条）。

個人情報保護法をごく単純化しますと、個人情報を利用する場合には、①その利用目的をできる限り特定した上で（同法15条）、②その利用目的の達成に必要な範囲でのみ（同法16条）、本人に利用目的を通知しつつ利用（同法18条）すること、③個人情報を取得する際には適正な手段で行う（同法17条）こと、をそれぞれ求めるというのが、基本的な構図となっています。また、個人情報を個人データとして整理した場合には、④個人データの第三者への提供は、原則として本人の同意なく行ってはいけない（同法23条）、という点が重要になります。よく出くわす、「個人情報だから教えられません」という場面は、この「第三者提供の制限」に関係します。

以上が遵守されるならば、映像が個人情報にあたるとしても、その利用は、個人情報保護法上、まったく問題なく可能です。

①利用目的の特定
②目的達成のために必要な範囲での利用・本人への通知
③適正な取得
④個人データの本人の同意を得ない第三者提供の制限

ところが、実は、個人情報保護法が定めるのはここまでです。①特定される利用目的の許容限界や、②「目的達成に必要な範囲」の具体的基準などについては、何も定めていません。そのため、極論すれば、いやがらせ目的で隣人の動向監視のために隣人宅を撮影しようとした場合、カメラの設置に際して、①「隣人の監視」として目的を特定し、②その目的達成に必要な範囲でのみ映像を利用し、その利用目的を本人に通知し、③隠し撮りでなく撮影し、④第三者提供もしないのであれば、個人情報保護法上は「適法」であることになります。

もちろん、その隣人は抗議するでしょうし、社会一般の常識としても、そういった利用は許されないと考えま

す。この常識的判断、すなわち利用態様の限界を画するのが「プライバシーの保護」なのです。個人情報保護法との関係では、①特定された利用目的の正当性の有無、②「目的達成に必要な範囲」の具体的な解釈が、「プライバシーを不当に侵害しないか否か」という観点で判断されるわけです。

「個人情報の保護」と「プライバシーの保護」は、次元を異にする問題です。また、プライバシーは、きわめて錯綜した概念ですが、この文脈では、個人の一定領域の情報をみだりに取得・利用されないことで、私生活の平穏を確保する、という意味合いで理解しておけば十分でしょう。

そして、目的が不当、あるいは、利用が必要な範囲を超え不適切と判断された場合、プライバシーの不当な侵害が生じていることになります。その場合、公序良俗違反（民法90条）となり、不法行為（同法709条）による損害賠償責任等が生ずることになります。

そもそも、民間の防犯カメラの設置・使用の根拠は、民法上の所有権（同法206条）や施設管理権などに求められます。個人情報保護法は、個人情報を取り扱うことの「根拠」規定ではなく、扱い方のルールを定めたものです。そういった点も含め、カメラ映像が個人情報に該当することになるといっても、従来からの適切な利用態様であれば、基本的には適法性が認められ、従来どおり許容されるのです。

3.生体認証機能の利用・許容限界

顔認証など生体認証機能を備えた防犯カメラシステムの許容性についても、個人情報保護法の次元とプライバシー保護の次元とで考えることになります。

プライバシー保護の観点から検討しましょう。顔認証機能付きのカメラシステムには、「プライバシーに対する影響が懸念される」とする指摘が、よくなされます。ただその場合、具体的にどういう事態が懸念されるのかは、実は明らかではありません。たとえば、万引き常習犯と疑われる者が来店した際、それを記憶している「警備員の目」で認証するのと、顔認証システムで認証することで、ただちにプライバシーへの影響に差が生ずるわけでもないでしょう。また、「行動監視につながる」という懸念であれば、生体認証システムの利用そのものではなく、認証用のデータ（個人識別符号）の共同利用が許されるか、という問題であるようにも思います。しかしながら、抽象的な印象論に終始しているのが現状ではないでしょうか。

こういった曖昧さは、個人情報保護法上の適法性判断にも影響を及ぼします。生体認証機能付きであっても、それを防犯に使うのであれば、①防犯での利用という、利用目的の特定については、従来のシステムと変わるところはないはずです。他方で、②従来のシステムに加えて、生体認証機能を備えたシステムの利用が、防犯目的の達成に必要な範囲での利用と認められるか、という点には、プライバシーの観点での議論が曖昧であることもあり、社会一般のコンセンサスが得られていないのが現状でしょう。これが、具体的な許容限界が明確にならない、1つの要因であるといえます。

今後は、防犯カメラ条例やガイドラインなどで、こういった高度な機能の許容限界について、具体的な例示がなされることが望まれます。その一例が、2016年10月に策定された宮城県の防犯カメラ設置ガイドラインです。また、個人情報保護委員会にも、許容限界に関する具体的な指針を示すことが望まれるところです。

また、顔認証システムがプライバシー保護の観点からも利用できるとの判断がされた場合、特に、生体認証に用いる個人識別符号については、それをデータベースに6か月以上保存するのであれば、保有個人データに該当することになります。もっとも、個人情報保護法施行令4条2号や4号に基づき、保有個人データ該当性が否定される可能性はあります。

他方で、こういった生体認証システムの利用に不安を感じる消費者に対しては、たとえば、認定個人情報保護団体制度に基づき、苦情に対して丁寧に対応し、不安を払拭する枠組みを構築することが望まれます。

4.マルチ・ユースへの要望と対応

また、生体認証機能等を備えたカメラシステムを、防犯のみではなく、商用に使うという「マルチ・ユース」へのニーズも、今後増加が予想されます。

こういった利用の許容性も、基本的には、防犯カメラの場合と同じ枠組みで判断されます。個人情報保護法上は、①「商用」のより具体的な目的を特定し、②その目的達成に必要な範囲であれば、基本的には許容されることになります。ただ、現時点では商用での街頭設置カメラ映像の利用は、まだ「社会常識」とはなっていないため、設置表示など、利用目的の通知はより丁寧に行うことが求められるでしょう。

また、②特定された目的が、個人識別性がなくても、たとえば、単なる人数分析や年齢・性別と行った属性分析でも達成できるのであれば、個人識別性を除去した

映像を用いるべきことになります。その意味で、マルチ・ユースに用いる場合のカメラシステムは、技術面も含め、より複雑になる可能性があります。

さらに、プライバシー保護の観点で考えると、現状では、防犯目的での個人情報の利用に比較して、商用での利用については、世論の抵抗感はより強い状態にあるように思われます。そうであれば、その利用についても、相応の慎重な検討が必要となるでしょう。

5.防犯活動しての映像の利用

近年、窃盗が疑われる者の映像を、顔にモザイクをかけてインターネット上に公開し、そのモザイクを除去しないこととの引き換えに盗品の返還を求める、といった事案が散見されるようになっています。

これは、防犯カメラ映像の利用としては、許容されるものではありません。犯人の検挙や盗品の取り戻しを自ら行うのは、現代の法治国家では原則として認められない「実力行使」「自力救済」にあたりかねません。個人情報保護法上も、「窃盗が疑われる者」の個人情報を、本人の同意を得ないで第三者提供（公開）することは、法令に基づく捜査の一環、その他警察からの問い合わせへの対応としての警察への提供以外は、基本的に認められません。防犯カメラ映像の「防犯という利用目的の達成に必要な範囲」としては、それが基本となります。

他方で、窃盗が発生しないようにする「戸締まり用心」は、私人が自ら行うべき事項です。防犯カメラ映像を不審者の早期発見、警戒のために設置者自ら使うことは、従来からある「鍵掛け」による防犯を、さらに進めたものとして認められることになります。とりわけ、転売の容易性や換金性が高まる中、被害額が1億円単位に達するような組織的集団窃盗など、「万引き」という範疇にはとどまらない甚大な被害も生じていますし、「自ら行う犯罪対策」への店舗側の要請も強まる一方です。

その要請に応えるため、たとえば顔認証機能の利用が認められるかの判断は、個人情報保護法上許容できる枠組みでも、最終的には、それを世間が納得するかという社会の常識に求められます。それは、プライバシー保護、言い換えれば、私生活の平穏確保に関する社会常識がどこに求められるかの判断です。

しかも、この「社会の常識」は状況によっても変化します。2008年にスタートしたGoogleのストリートビュー・サービスは、当初はプライバシー侵害を懸念する声も大きかったのですが、現在では、広く受け入れられています。また、店頭での顔認証機能付きカメラシステムの導入には、「行動監視されたり、趣味・趣向が丸裸にされるのでは」との懸念が一部でなされますが、他方で、店舗での購買履歴等が記録されるポイントカードの利用や、あるいは、ネット通販等の閲覧・利用履歴が事業者に把握されることについて、躊躇の声は少ないようです。

社会の常識、納得感の見極めには、たしかに困難な面があります。それが、この問題の解決の方向を見えにくくしているのです。

6.まとめに代えて

顔認証機能なども含めた、高機能化した街頭設置カメラシステムの利用がどこまで認められるかについては、2つの次元で考えるべきことになります。

第1は、撮影される映像や個人識別符号に個人情報該当性が認められることを前提に、個人情報保護法の規定を遵守することです。そうであれば、個人情報保護法の枠組みにおいても、その利用は適法なものとなります。これが、必要最低限です。

第2に、個人情報保護法上許容されるとしても、その利用が社会的に許容されるかは、社会がプライバシー保護として何を求めるか、という「社会の常識」にかかってきます。それは、犯罪状況にも左右されるし、プライバシーとして具体的に何を求めるのか、現実空間とサイバー空間とでの認識の相違など、より複雑な方程式になっています。

その判断は、最終的には、ⓐ高機能なカメラシステム等を利用することに得られる利益、ⓑそれがプライバシーの利益に及ぼす影響がどの程度なのか、であり、それを丁寧に説明するという透明性の確保が何より重要です。ストリートビューが受容されたのも、撮影された者が撮影内容を確認できるという意味で透明性がより確保されやすく、被撮影者自身も他の場所の撮影データを利用することで利益を享受できるシステムであった面も大きかったと考えられます。

そして、その両者の比較衡量から、ⓑがあるとしても一定程度にとどまり、ⓐがより優越することに、社会一般の理解が得られるかという点に、そのシステムの利用が許容されるかの判断がかかってくるのです。

本講演は、科学研究費助成事業（基盤研究（C）・研究課題番号:26380095）による研究成果の一部を反映したものです。