捜査機関データ保護指令の仮訳の公開

2019 年 11 月

JCLU では、2016 年 4 月 27 日、EU 議会において可決され、同年 5 月 5 日に発効（施行）された捜査機関データ保護指令（以下「本指令」）について、日本における捜査機関の個人データの取り扱いの抜本的な見直しをする際の大きな参考になると考え、本指令を前文とともに全訳し、ウェブにおいて公開することといたしました。

なお、本訳は仮訳であり、随時修正・変更されます。誤訳等にお気づきの場合は、以下のメールアドレス（jclu@jclu.org）にご連絡ください。本訳の著作権は JCLU に帰属します。また、誤訳等の責任は負いません。何卒ご了承の上ご活用いただければ幸いです。

１　概要

捜査機関データ保護指令（「本指令」）とは、正式名称を、「犯罪の予防、捜査、取り調べ若しくは起訴、又は刑罰の執行を目的として、所轄官庁により実施される個人データの処理に関する自然人の保護、並びに当該データの自由な移転に関するＥＵ指令」といいます(1)。GDPR と同日に EU 議会において可決・施行されました。

GDPR が民間企業や政府機関による個人データの取扱に関するルールを定めたものである一方、本指令は、主に捜査機関による個人データの取り扱いに関するルールを定めたものです。

GDPR が Regulation（規則）であるのに対し、本指令は Directive（指令）です。EU 法制度において、「規則」（Regulation）は、EU 議会における施行と同時に、加盟国の政府や企業、個人に直接効力が及びます。また、加盟国の国内法に優先します。他方で、「指令」(Directive)は、加盟国の政府に対して、国内立法等の措置をとることにつき、法的拘束力を及ぼしますが、企業や個人には直接適用はされません。措置の具体的な内容は加盟国政府に委ねられます。

２　特徴

本指令は、犯罪の予防や捜査に求められる密行性や取扱情報の機密性と、個人データ保護の重要性のバランスを調整するものです。最大の特徴は、デジタル時代の情報の特殊性を適切に評価する点です。

例えば、適用範囲として、「全部か一部かを問わず、個人データの自動処理に適用される。また、ファイリングシステムの一部を構成し、若しくはファイリングシステムの

---

(1)　2016年4月27日 欧州議会及び欧州理事会指令2016/680
DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016
on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

一部とすることを意図された処理については、自動処理でなくとも適用される。」（2 条 2 項）として、個人データのコンピュータ処理を明文で対象としています。

また、個人データの定義も、GDPR と同様に、「識別された、又は識別可能な自然人（「データ主体」）に関するあらゆる情報をいう。識別可能な自然人とは、氏名、識別番号、位置データ、オンライン ID のような識別子、又はその人物に特有の物理的、生理的、遺伝子的、精神的、経済的、文化的、若しくは社会的な要素を 1 つ又は 2 つ以上照合することによって、直接又は間接的に識別されうる自然人のことをいう。」（3 条 1 項）と、データマッチングを念頭において、幅広く保護の対象としています。

規制対象となる捜査機関等の「処理」行為については、「自動化された手段か否かを問わず、個人データ又は個人データの集合に適用されるあらゆる操作又は一組の操作を意味する。例えば、収集、記録、編成、構造化、保存、改変若しくは変更、抽出、参照、利用、送信による開示、公表若しくは公表を可能なものにすること、整列若しくは組み合わせ、制限、消去、又は破壊が挙げられる。」（3 条 2 項）と、コンピュータによる処理用語が列記されています。

デジタル時代においては、些細なデータであっても大量に保存・収集し、かつ処理能力の極めて高いコンピュータでデータマッチングすることが可能となったため、犯罪が起きてから、事後的にあらゆるデータの足跡を照合することで、個人の言動や嗜好を詳細に分析することが可能となっています。捜査機関が現代技術を野放図に利用することで、個人の自然権・プライバシーが侵害されないよう、本指令は、幅広いデータやその処理を規制の対象としています。

規制の方法も現代的です。例えば、25 条では、自動処理システムにおける個人データの収集、変更その他の利用について、処理操作の理由及び日時等が確定でき、かつ可能な限り個人データの参照者や個人データの受領者を特定できるようにログを残すことを求めています。そして、監督機関から要請があった場合には、このログを開示しなければならないこととしています。

捜査機関の活動は秘匿性が高いため、それを公にしたり、捜査対象者に広く開示する仕組みを取り入れることは困難ですが、監督機関という独立した第三者機関の目が及ぶようにすることで、捜査活動の適切性を確保しようとしていることがわかります。

監督機関は、個人データの取扱いについて調査を行い、違反を当局に通告する権限も有しています。このような監督機関は各加盟国に設けることとされ、本指令に基づく職務遂行と権限行使は、完全に独立していなければならないとされています。この監督機関の構成員の任命は透明性のある手続きによることとされ、加盟国は法律によって監督機関の設立や構成員の資質や適格性、任命に関する手続などを法律によって定めなければなりません。秘匿性の高い情報やセンシティブな情報を扱うため、監督機関の構成員や職員には、秘密保持義務が課されています。

強い権限があり、かつ独立性の高い監督機関が監督することによって、犯罪の予防、捜査と、個人データの適正な取り扱いのバランスをとっているのです。

3　日本における意義

GDPR が、主に EU 領域における個人データの保護を目的としながら、域外移転の規制や EU 市民の個人データの取り扱いの規制などを通じて、EU 域外の主体にとっても重要な意義を有するのと同様、本指令も、EU 域外の主体にとって重要な意義を有します。なぜなら、本指令は、日本の捜査機関など EU 域外の捜査機関が、EU 域内の捜査機関と捜査情報を共有する場合などにおいて、本指令と同水準の個人データ保護の制度を採用することを条件としているためです。

日本では、行政機関個人情報保護法が、捜査機関の保有する個人情報の取り扱いのルールを定めていますが、捜査に関する情報には適用除外が多く認められており、個人データの保護に関し、本指令の水準とは大きな差があるのが現状です。

GDPR は、EU 域外の国が EU と同水準の個人データの保護制度を整えている場合に、原則として域外移転を認める制度(いわゆる十分性認定制度)を設けています。2019 年 3 月、日本は十分性認定を受けましたが、その際には、日本の捜査機関の個人データの取り扱いについて、事実上改善を求める附則が採択されました。

また、民間企業としても、本指令の水準に満たない捜査機関に対し、安易に個人データを共有すると、GDPR 違反を指摘される恐れがあります。

4　終わりに

デジタル時代のプライバシーの重要性は高まる一方です。民間において、GDPR の枠組みは浸透しつつあり、適切な個人データの取り扱いが実現されつつあります。他方で、捜査機関をはじめとする政府における個人データの取り扱いは、いまだに古い枠組みに囚われたままとなっています。

本訳が、このような状況を改善する一助となることを期待しています。

以上