Chinese Business

Q&A 中国ビジネス Q&A 情報化社会における企業による個人情報取

Q **現在、情報技術、インターネット技術の急速な発展・普及に伴い一般市民に利便性がもたらされると同時に、個人情報の保護という、より大きな問題にも直面しています。個人情報の流出やその侵害に関連する事件のニュースもよく見受けられます。2017年6月に「サイバーセキュリティ」法が施行されたことで、個人情報および重要データの中国国内での保存や中国国外への送信に当局の審査（クロスボーダーセキュリティ評価、以下「セキュリティ評価」）等の厳しい規制が課され、中国ビジネス関係者からの大きな反響を呼びました。**

このような状況を背景に、ネット時代に相応しい個人情報保護制度を構築すべく、中国当局はここ数年の間に個人情報保護に関する多くの法令を制定し、その執行を強化する対策を多方面で講じ、ネット社会における個人情報の保護を推進しています。これらの法令、特に中国で事業展開するうえでの個人情報を含む種々の情報やデータを中国国外へ送信する行為への法規制は、どのような内容となっているのでしょうか。外資系企業としては、どのように対応し、どのような点に注意すればよいのでしょうか。

A

1. 個人情報保護に関する基本的な法体系

中国では、個人情報保護法の基本法が定められていないのが現状であり、個人情報に関する規定は法律、行政法規、司法解釈、部門規則、政策に散見される状態になっています。

そのうち、09年の刑法第7次改正案では初めて公民個人情報侵害罪が新設され、これを契機に個人情報の立法が加速化しました。13年改正の「消費者権益保護法」29条、15年の刑法第9次改正案による公民個人情報侵害罪に関する規定の改正、今年3月に公布された民法総則111条、今年5月8日に公布・施行の「公民個人情報侵害刑事事件の取扱いにおける法律の適用に係る若干の問題に関する最高人民法院および最高人民検察院の解釈」（以下「本司法解釈」）、今年6月1日施行の「サイバーセキュリティ法」等の個人情報保護に関する重要法令の立法が続き、こうして個人情報保護の法的基礎がある程度確立されました。

●●●

2. 個人情報保護をめぐる法規制の最新動向

ここ数年に施行された各法令により個人情報保護は確実な一歩を踏み出しつつありますが、その最新動向につき以下に概要を論じます。

（1）民法総則による民事法における個人情報権利の明示

これまでの民事関連法令は個人情報の保護を明確に定めておらず、権利侵害責任法等の法令を通じプライバシー権として法的保護を与えていましたが、今年10月1日施行の民法総則111条では、自然人の個人情報は法的保護を受ける旨が定められ、実務上において重要な意義を有しています。今後、身分証明書番号等の個人情報が侵害された際には、プライバシー権侵害に基づく主張・請求ではなく、個人情報権侵害を主張し、侵害差止めや損害賠償等の民事的な請求を行いうると解されます。

（2）刑法第9次改正案および司法解釈による個人情報侵害の刑事規制――公民個人情報侵害罪の明確化

刑法第9次改正案は253条1項の公民個人情報侵害罪について、「国の関連規定に違反し、他人に公民の個人情報を販売、または提供し、情状が重い場合、3年以下の有期懲役または拘留に処し、罰金を単科または併科する。情状が特に重い場合、3年以上7年以下の有期懲役に処し、罰金を併科する。国の関連規定に違反し、職責の履行またはサービス

扱いの最新動向と注意点

金杜法律事務所（King&Wood Mallesons）中国弁護士
中国政法大学大学院 特任教授　劉新宇

提供の過程において取得した公民の個人情報を他人に販売または提供した場合、前項の規定により処罰する。窃取またはその他の方法で違法に公民の個人情報を取得した場合、第1項の規定により処罰する。単位[注1]が前3項の罪を犯した場合、単位に対して罰金を科し、かつその直接に責任を負う主管者およびその他の直接責任者に対して、各項の規定により処罰する」と定めています。

なお、「公民の個人情報」、「他人に提供する」、「その他の方法で違法に取得する」とはそれぞれどのような定義なのか、「情状が重い」とはどのような基準で判断されるのか、これらの不明な点については、本司法解釈が全面的かつ体系的な規定を明確に定めたうえで解説しています。

（3）「サイバーセキュリティ法」によるサイバーセキュリティ強化に伴う個人情報保護の強化

本司法解釈と同時に施行された「サイバーセキュリティ法」は、初めて法律の次元で「個人情報」の概念を明確に定め、個人情報保護の主要義務についても、本司法解釈に相当するいくつかの条項を設けて定めています。

「サイバーセキュリティ法」の施行に関して、同法37条に定める重要情報インフラ運営者の個人情報および重要データの中国国内での保存や中国国外への送信時の当局によるセキュリティ評価等の厳しい規制への適正な対応が最も注意すべき点となります。しかし、このセキュリティ評価制度にかかる「重要情報インフラ」の具体的な範囲、セキュリティ評価が必要とされる個人情報および重要データの範囲、セキュリティ評価のプロセス、評価要点、評価方法については同法に具体的な定めがなく、現在意見募集が行われている一連の下級法令の意見募集稿または草案（「重要情報インフラセキュリティ保護条例（意見募集稿）」、「個人情報および重要データ出国セキュリティ評価弁法（意見募集稿）」のほか、全国情報安全標準化技術委員会による「情報安全技術・データ国外移転（原文「出境」）セキュリティ評価指南（草案）」等）に着目しなければなりません。これらの条例・弁法・指南は、まだ草案または意見募集の段階ですが、いずれもセキュリティ評価の問題について一定の方向性を示しているため、その正式な公布が待ち望まれます。

●●●

3. 個人情報を取扱う企業の注意点

個人情報を取扱う企業においては、従業員の個人情報、顧客情報の収集・利用に対し一層の注意を払う必要がある一方、違法な情報の取得を避けるため相応の社内措置・対策をとる必要もありますので、その注意点および対策について述べます。

（1）個人情報の定義範囲および行為基準への注意

「サイバーセキュリティ法」と本司法解釈における、個人情報の保護範囲および違法・犯罪行為の基準に関連する定めに照らし、企業として注意すべきポイントについて、整理します。

①個人情報の定義と範囲

「個人情報」とは、「サイバーセキュリティ法」76条によれば「電子またはその他の方式で記録された、単独でまたはその他の情報と組み合わせて自然人（個人）の身分を識別できる、自然人の氏名、生年月日、身分証明書番号、個人の生体認証情報、住所、電話番号等を含むがこれらに限らない各種情報をいう」と定義されています。その定義の中心的要素は、個人の身分の識別であることがみてとれる一方、本司法解釈は、「特定の自然人の身分を識別することができる情報」のみならず、行動の目的地・軌跡等に関する記録、活動状況を反映した情報も公民の個人情報であると初めて定められ、広い解釈をしていると考えられます。もっとも、これら2つの法令のいずれに従って「個人情報」を認定するのか、企業による個人情報侵害行為が成立するのかについては、各政府主管部門によって解釈・判断が異なる

（本文は31頁に続く）