『個人情報保護法』施行による企業コンプライアンスへの影響及び提案

中国弁護士　李　蕾　中国弁護士　虞　文隆
翻訳・編集　朱　彤　翻訳・編集　呉　穎奇

要　約

中国の『個人情報保護法』が 2021 年 11 月 1 日より施行されている。『個人情報保護法』は、個人情報に関する保護を強化するとともに、中国の国内企業だけではなく、中国でビジネスを営む外国企業にも適用される可能性があるという点で注目を集めている。

本稿では、『個人情報保護法』のポイントを紹介し、実例を交えながら、『個人情報保護法』に関する企業側の実務的な考え方、個人情報を取り扱う際の注意点をまとめ、『個人情報保護法』の限界および展望を考察する。

目次

1．はじめに

モバイルネットワーク技術の進化に伴い、中国ではインターネットが人々の日常生活に浸透している。これを受けて、個人情報の保護は重要な課題となってきた。中国インターネット情報センター（CNNIC）の調査データ(1)によると、2021 年、個人情報漏洩に遭った中国ネットユーザーの割合は約 22%である。

しかし、中国には長期にわたって、個人情報の保存と転送に関する効果的な規制がないため、個人情報の改ざん、悪用及び営利を目的とする違法転売が多発している。また、それに伴う通信ネットワーク詐欺、スパムメッセージが深刻な問題となっている。さらに、スマートフォンの普及に伴い、モバイルアプリによる個人情報の過剰収集とスパム広告の氾濫が浮き彫りになってきている。

本稿では、『個人情報保護法』のポイントを紹介し、中国の司法実践により、『個人情報保護法』施行による企業が直面するコンプライアンスへの影響を考察し、アドバイスを助言する。

2．中国における個人情報に関する基本制度

2012 年、中国では『オンライン情報の保護強化に関する決定』が全国人民代表大会によって可決され、「国家は、国民の個人情報を識別し、個人のプライバシーを保護できる電子情報を保護する」ことを明確にした。個人情報保護の要件が法的なレベルで確認されたのはこれが初めてであり、「合法性、正当性、必要性」の原則も決定され、その後の法律で援用および確認された。

また、2016年に公布された『サイバーセキュリティ法』では、データ漏洩等が発生したとき、ユーザーへの通知が新たに義務化された。

そして、『中華人民共和国個人情報保護法』（便宜上、以下『個人情報保護法』という）が2021年8月20日に第13期全国人民代表大会常務委員会第30回会議で可決され、2021年11月1日より施行されることになった。この『個人情報保護法』は中国初の個人情報保護分野の専門法であり、303日間にわたる3回の全国人民代表大会での審理を経て公布に至った。この『個人情報保護法』では、データ漏洩時の通知義務についてより具体的な規定がなされ、通知が必要となる具体的な状況、通知の対象などの内容が加えられた。

『個人情報保護法』は、先の『データセキュリティ法』、『サイバーセキュリティ法』とともに、中国のデータセキュリティ、サイバーセキュリティ分野の法的枠組みを構成するものである。

3.『個人情報保護法』のポイント

（1） 個人情報定義の拡大

『中華人民共和国民法典』（以下『民法典』という）における個人情報とは、電子またはほかの方法により記録された、単独またはその他の情報と結合した形で、特定の自然人を識別することのできる各種の情報のことである。

『サイバーセキュリティ法』における個人情報とは、電子またはほかの方式により記録された、単独またはその他の情報と結合した形で、自然人の身分を識別することのできる各種の情報のことである。

『民法典』において、個人情報を「自然人を識別することのできる情報」と定義し、『サイバーセキュリティ法』においては、「自然人の身分を識別することのできる情報」と定義している。両者の定義はほぼ一致している。

『個人情報保護法』における個人情報とは、電子またはほかの方法をもって記録された、すでに識別されており、または識別可能である自然人に係る各種の情報のことである。すなわち、「自然人を識別することのできる情報」のみならず、「識別済または識別可能な自然人に関わる識別性以外のほかの各種の情報」も含まれている。ただし、匿名化処理後の情報は含まれていない。

よって、『個人情報保護法』は、『民法典』及び『サイバーセキュリティ法』と比べて、個人情報の定義を拡大し、さらに、適用範囲と保護を最大化し、『民法典』及び『サイバーセキュリティ法』と組み合わせながら、個人情報への保護を強化する。

（2） 個人情報の「削除」

『個人情報保護法』は、『民法典』に規定された個人情報の収集、保管、使用、加工、伝送、提供、公開等の情報処理行為に、「削除」を新たに加えた。さらに、「国家機関、法律法規により授権された公共事業組織または営利法人、非法人組織および自然人は、個人情報処理活動において『個人情報保護法』に適用し、法律が規定された状況を除外する」と明記している。

個人情報の削除は、プライバシーを保護するだけではなく、『民法典』に規定された個人情報操作の各権限に対する補完でもある。

（3） 域外適用の原則

海外企業は、インターネットを通じて、世界各地のユーザーに商品またはサービスを提供することができる。そして、中国人ユーザーが利用すれば、中国人の個人情報の収集と処理が発生する。以前の法律法規では、行政監督においても、刑事処罰においても、中国の領域外における中国人の個人情報の収集、処理を有効的に管轄することができなかった。そのため、中国国内の自然人の情報流出等によるセキュリティ面でのリスクがあった。

そこで、「個人情報保護法」では、域外適用の原則を策定し、「中国国内の自然人の個人情報を処理する活動であるならば、中国国内または中国領域外の組織または個人に対して、いずれも本法は適用される」と規定されている。これまでの法規制の効力範囲を超え、中国領域外の主体の特定行動にまで拡大した。

（4） 告知及び同意原則

『個人情報保護法』によると、個人情報処理者は個人情報を処理する際には、個人に知らせ、かつ個人からの同意を得なければならない。具体的には、個人情報処理者は、個人情報の処理前に、明瞭な方式、わかりやすい言葉で偽りなく、正確に、完全に法により定められた各事項を個人に知らせなければならない。

『個人情報保護法』では、上記の同意について、「個人が状況を充分に理解している前提で自発的かつ明確

に行わければならない」と明記している。それから、個人情報処理者は個人情報を処理する際、個人に告知しなくてもよい状況を二種に限定した。一種目は、秘密保持が必要あるいは告知が不要な状況を規定した法律、行政法規がある場合。二種目は、緊急事態下において自然人の生命、健康及び財産の安全を保護するための個人への適時告知ができない場合、である。ただし、緊急事態解消後、速やかに告知しなければならない。上記の二種の場合を除き、個人はその個人情報の処理に対して完全、かつ充分な知る権利を有する。

（5） 顔認証技術の規制強化

ビッグデータと人工知能技術の急速な発展により、公共の場所に画像収集及び個人身分識別装置を取り付けることで、自然人の顔の特徴など生物識別情報及び移動軌跡などの情報を随時処理することが可能となった。

『個人情報保護法』の定めによると、公共の場所に画像収集や人物特定の設備を設置する場合には、公共の安全維持のために必要で、国家の関連規定を遵守し、かつ明瞭な注意喚起の表示を設けなければならない。こうして収集した個人の画像、人物特定情報は、公共の安全維持の目的のみに使用することができ、その他の目的に使用してはならない（個人から個別の同意を得た場合を除く）。

例を挙げると、中国政府は、道路、地下鉄、住宅地などの公共の場所に、画像や人物特定情報を収集するためにカメラを大量に設置しているが、公共の安全維持のためであり、他の目的には使用していない。そのため、上記の行為は『個人情報保護法』の関連規定に準拠している。緊急事態以外では、企業、社会組織、個人は、人物特定情報を収集してはいけない。

（6） 個人及びその近親者の権利

『個人情報保護法』には、個人情報活動における個人の権利が明記されている。

具体的にいうと、その個人情報の処理に対して知る権利、決定する権利；個人情報の照会、複製を求める権利；個人情報処理者へ個人情報の移転を求める権利；不正確或いは不完全な個人情報の修正、追加を求める権利；個人情報の削除を求める権利；個人情報処理規則の解釈、説明を要求する権利、である。

また、死亡者の近親者の合法的、正当な利益の保護と死亡者本人及びその交際者のプライバシー及び通信秘密の保護を両立するため、『個人情報保護法』では、自然人が死亡した場合、その近親者は、死亡者に関する個人情報について照会、複製、修正、削除などの権利を行使することができる。ただし、死亡者が生前に別の段取りを行っている場合を除く。

（7） 個人情報侵害事件における過失の推定規定の適用

『個人情報保護法』では、「個人情報の処理が個人の権益を侵害し、損害をもたらした場合、過失の推定を適用する」と規定している。個人情報処理者は、自身に過失がないことを証明できないかぎり、損害賠償などの権利侵害責任を負わなければならない。

過失の推定規定の適用により、被害者の立証負担が軽減される。また、損害賠償については、財産的損失であれ、精神的損失であれ、個人がこれにより受けた損失あるいは個人情報処理者がこれにより得た利益に基づき算定する；算定が困難な場合は、実際の状況に基づき損害額を確定する。

4.『個人情報保護法』の運用に関する実務的な考え方

法律法規を遵守することは、コンプライアンス上のエンドラインである。企業は『個人情報保護法』の規定に依拠し、自らの情報管理体制を見直し、データコンプライアンスを展開する。

ここでは、具体的なケースを想定し、企業が内部管理および経営活動において注意すべき点、リスクとコンプライアンス対策について解説する。

（1） 内部管理における義務

ケース１：とある化粧品会社では、従業員を募集する際に、住所、同居人、学歴、配偶者の有無などの情報を含むフォームの記入を求めている。

上記のケースでは、個人情報の収集は必要限度を超えている。『個人情報保護法』の施行により、従業員の個人情報を過剰に収集する行為は合法性に欠ける。面接等の採用プロセスにおいても応募者の個人情報を過剰に収集してはならない。

『個人情報保護法』５条、６条には、「個人情報の処理は、合法、正当、必要、誠実の原則に従わなければならない」と、「個人情報の処理は、明確かつ合理的

な目的を持ち、処理目的に直結して、個人の権益に最小限の影響を及ぼす方法をとるべきである」と規定されている。

また、『労働契約法』8条によれば、雇用者が労働者を募集、採用する場合は、労働者の労働契約に直接関係する基本的状況について知る権利を有し、労働者は事実のとおりに説明しなければならない。雇用者は、労働者の職務に関係する個人情報について知る権利を有する。収集方法は、面談や、労働者の自主的提供、バックグラウンドチェックなどがある。

したがって、会社の人事担当者は、面接時に、応募者に学歴、住所など職務に関係する情報のみを収集することができ、書面または口頭などの形式で同居人、結婚の有無などの職務に関係のない情報を収集してはならない。

企業の人事部門が個人情報を収集・管理する部門であるため、『個人情報保護法』の施行により、人事部門は一番影響を受ける部門である。従業員と企業の立場は不平等であるため、多くの人事部門は、個人情報を収集する際に法規制を厳格に遵守することを怠っている。また、従業員も、自身の正当な権利の保護に注意を払っていない。人事部門は、個人情報を収集する前に従業員から明示的な許可を得なければならない。

以上のように、企業側は、情報を収集する際に、従業員の個人情報の取得範囲が「必要性」の原則、すなわち、労働契約に直接関連する基本的な状況に限定され、その他の非必須個人情報については、労働者の意思を尊重し、可能な限り取得しないことを留意すべきである。

ケース2：とある市場コンサルティング会社では、出張や外勤中の従業員の行動を監督するため、位置情報共有アプリやPDA[(2)]などのGPS測位方法を通じて、従業員の行動を把握している。コロナの影響により、多くの労働者がテレワークを余儀なくされる中、GPS測位による監督措置が広がっている。

このケースについては、『最高人民法院と最高人民検察院による公民の個人情報侵害刑事事件の審理における法律適用の若干問題の解釈』1条により、「移動履歴」は「公民の個人情報」に属し、従業員の正確な位置情報を監視することは、個人からの同意を得ていない場合、従業員のプライバシーを侵害する疑いがある。

さらに、多くの企業は、勤怠管理システム、業務管理ソフトウェアまたは財務管理システムなどの第三者サービスを使用する際に、合理的な業務目的で、サプライヤー、関連会社、顧客などの第三者に従業員の個人情報を開示、提供することがある。その場合、従業員の個人情報を開示、提供する前に、従業員の同意を得ることに留意すべきである。

（2） 経営活動における義務

ケース3：とある小売企業は、店舗内に設置したカメラやセンサーを通じて収集した顧客情報を画像解析技術で処理し、購買行動を分析する実験に使っている。具体的には、主に顔認証技術により、顧客の特徴、年齢、身長、性別などの情報を収集し、その情報に基づき顧客の消費意欲を分析する。

このケースの場合、『個人情報保護法』26条により、公共の場所において画像収集、人物特定設備を設置する場合、明瞭な注意喚起の表示を設置しなければならない。収集した個人の画像、人物特定情報は、公共の安全維持の目的のみに利用することができ、その他の目的に使用してはならない。（個人から個別の同意を得た場合を除く。）

企業がマーケティングの目的で個人の顔の情報を収集する場合、店舗内で注意喚起の表示を設置するだけでは十分とは言えず、個人から個別の同意を得る必要がある。しかし、消費者から個別の同意を得ることは明らかに非現実的であり、企業はマーケティングのための顔認証技術の導入に対して慎重になるべきである。

ケース4：とある小売業界の企業は、個人情報を収集し、集積した顧客の履歴データに基づき取引価格などで差別的扱いをした。購買力の高い常連客に対し価格を釣り上げる、いわゆる「ビッグデータ殺熟」[(3)]行為である。

このようなケースの「ビッグデータ殺熟」は違法行為と見なされ、政府が規制に乗り出した。『個人情報保護法』24条によると、個人情報処理者が、個人情報を利用して自動的意思決定を実施する場合、意思決定の透明性及び結果の公平性、公正性を保証しなければならない。個人に対して取引価格などの取引条件について差別待遇を実施してはならない。したがって、企業は意思決定アルゴリズムを利用する際、個人の権益を侵害しないように注意しなければならない。

また、自動的意思決定[4]を通じて個人向けの情報配信、マーケティングを行う場合、個人に選択権と拒否権を保障する必要がある。即ち、その個人の特徴に適合しないオプションを同時に提供する、または個人に簡便な拒否方法を提供しなければいけない。

さらに、個人情報処理者は自動的意思決定を通じて個人の権益に重大な影響を与える決定を行う場合、個人は自動的意思決定のみによって行われた決定を拒否する権利を有する；個人が異議を唱える場合、個人情報処理者は人的な意思決定を行うことができる。

ケース5：とある個人が、常に利用している銀行Aとは別に、銀行Bに融資を申し込んだ。銀行Bは当該個人に、その銀行Aに保存されている信用状況、消費能力を裏付ける個人データの提供を要求した。これは、個人情報のデータポータビリティ権[5]に関する典型的なケースである。

データポータビリティ権は、照会及び複製の権利の重要な補足となる。また、データポータビリティ権について規定したのは中国においてはじめてである。

よって、このケースでは、当該個人が銀行Aに関連個人データの移転を求めた場合、個人の身元を確認したうえ、銀行Aはデータを持ち運び可能なものにして個人に提供する必要がある。現行法では、「ポータブルメディア」に対して定義しておらず、通常、電子データ等の形式は「ポータブル」の要求を満たすと見られる。

ケース6：とあるアプリの利用者は、手軽に利用するため同アプリが収集した個人情報を第三者のアプリに提供することを承認した。その後、当該利用者は第三者のアプリの利用を中止したため、その個人情報の提供を取消したい。

このケースでは、同アプリの運営会社は利用者からの承認取消の要求を受け取った場合、不必要または不合理な条件を設定してはならず、利用者の要求にスピーディーに応えなければならない。手動処理が必要な場合は、15日以内に検証と処理作業を完了する必要がある。

また、ユーザーは、個人情報の収集、使用、保存及び共有などの処理の全過程において、同意の取消を行える。同時に、企業は、個人に対して便利かつスピーディーな取消方法を明示しなければならない。

ただし、条文には「便利」と「スピーディー」に対して明確な定義をしておらず、実務上、「アプリによる個人情報の違法・反則な収集・利用の認定方法」の規定を参照することができる。事業者は、同意の取消に不必要または不合理な条件を設定してはならず、ユーザーの取消請求に迅速に対応しなければならない。人工処理が必要な場合、制限期間内（制限期間は15営業日を超えてはならず、制限期間がない場合、15営業日とする）に検証と処理を完了する必要がある。個人による同意の取消は、取消前の個人の同意に基づいて実施された個人情報処理活動の有効性に影響を与えない。企業は、取消前の個人情報についての処理活動及び結果を保持することができる。

5．個人情報を取り扱う際に注意すべき点

『個人情報保護法』の施行により、企業は個人情報を慎重に取り扱うべきである。個人情報の分類、収集、保存、アクセスまたは監督の各過程における各部門の役割分担、協調を明確にするべきである。具体的に、1. 個人情報の分類、2. 収集、3. 保管、4. アクセス、5. 管理、という五つの点に分けて解説する。

（1） 個人情報の分類

法務部門は個人情報の分類を担う。法務部は個人情報管理上のリスクを洗い出し、個人情報の分類に応じてコンプライアンス対策を作成する。

個人情報の分類とは、個人情報の属性または特徴に応じて、一定の原則と手法により個人情報を分類することをさす。主に個人情報の取り扱いに注意を要する程度、漏洩、乱用した際の影響に基づき分類する。企業は、属する業界をもとに、GB/T35273-2020「情報セキュリティ技術個人情報セキュリティ規定」と業界の標準に従い、分類を行うべきである。

「情報セキュリティ技術個人情報セキュリティ規範」により、個人情報は、センシティブ情報と一般的情報に分類することができる。

1） センシティブ情報

財産に関する情報：銀行口座情報、識別情報（パスワード）、預金情報、不動産情報、借入情報、信用情報、取引・消費記録、台帳記録、仮想通貨、バーチャルグッズ取引、ゲーム類の引換コードなどのデータ財産情報

健康に関する情報：医療関連記録。例：診療録、入院記録、医師指示票、検査報告書、手術・麻酔記録、看護記録、投薬記録、薬物・食品アレルギー情報、出産記録、既往歴、通院状況、家族歴、現病歴、感染症既往歴など

生体認証情報：DNA、指紋、声紋、掌紋、耳介、虹彩、顔識別特徴など

本人確認情報：身分証明書、士官証、パスポート、運転免許証、従業員証、社会保険カード、居住証明書など

その他の情報：性的指向、結婚歴、宗教・信仰、違法・犯罪事件の未公開記録、通信記録及び内容、アドレス帳、友だち・グループのリスト、移動履歴、ウェブ閲覧履歴、宿泊情報、正確な位置情報など

2） 一般的情報

一般的個人情報は、センシティブ個人情報以外の個人情報のことである。

センシティブ情報が漏洩した場合、個人のイメージ、評判、社会的評価に影響を及ぼす。センシティブ情報の分類は個人情報処理の第一歩であり、過去の経験ではなく、GB/T35273-2020「情報セキュリティ技術個人情報セキュリティ規定」などの業界標準を参照して分類しなければならない。

（2） 個人情報の収集

人事部門は、個人情報の収集を行う部門である。人事部は、策定した個人情報の分類に従い、収集を実施し、また保護戦略を作成する。

1） センシティブ情報について

『個人情報保護法』29条の規定により、センシティブな個人情報の取扱いは、個人から個別の同意を得なければならない；法律、行政規定がセンシティブな個人情報の取扱いに書面による同意取得を規定している場合、その規定に従わなければならない。

センシティブ情報が漏洩したり、違法に利用されたりすると、個人の人格権を侵害する、または、個人の人身、財産に危害を与える恐れがある。よって、企業は、個人から書面にて個別の同意を得てから、収集、取扱いをする必要がある。

2） 一般的情報について

『個人情報保護法』13条2項によると、個人を当事者の一方とする契約の締結、履行に必要である場合、または法に基づき制定した労働規定、制度及び法に基づき締結した労働契約に基づく人材管理の実施に必要である場合には、個人情報処理者は、個人情報を取扱うことができる。

一般的個人情報は、会社の経営や業務に必要であるため、企業はそれらを収集及び処理することができるが、他人に開示してはならない。

（3） 個人情報の保管

企業のIT部門は、個人情報の保管を実施する。IT部門は、収集された個人情報を適時に入力および保管し、また、個人情報を保管する過程で、個人情報の非特定化や匿名化等の措置を講じる必要がある。

『個人情報保護法』51条により、個人情報処理者は個人情報の保護のため、相応のパスワード設定、非特定化などの安全技術措置を実施する必要がある。

データの非特定化と匿名化は、情報取扱いにおける重要なプロセスである。非特定化とは、個人情報が、処理を経た後、ほかの追加情報に頼らなければ特定の個人が識別できない程度まで行う処理である。匿名化とは、個人情報が、処理を経た後、特定の個人を識別または関連付けることができず、かつ処理された情報を復元できない手法を指す。

IT部門は以下の方法によって個人情報の非特定化または匿名化を実現する。

①個人情報を伝送と保存する際、パスワードをかけるといった安全措置を取る；
②個人識別情報と個人身分情報を別々に保存する；
③個人情報の保存期間は、個人情報主体の利用許可の目的を達成するために必要な最低限の期間とする。
④個人情報収集の前提がなくなった場合は、速やかに収集を中止する。

個人情報の保管のコンプライアンス管理は困難であり、従業員から漏洩する可能性がある。つまり、個人情報保管の鍵は漏洩防止である。暗号化と解析の手続きを複数人に分かれて管理し、保管段階での漏えいを防ぐ。また、仮に漏えいしたとしても、個人情報が解析できないため、損失を最低限に抑えることができる。

（4） 個人情報へのアクセス

IT 部門は、『個人情報保護法』の関連規定に基づき、個人情報処理者は個人情報への不正アクセスを防止しなければならない。

具体的には下記のとおりアクセス権限を設定することができる：

①「最小権限の原則」に従って、社員に業務を遂行するために最低限の権限を与える；

②個人情報について修正、コピーまたはダウンロードといった重要な処理を行う場合、承認手続きと作業ログを設置する；

③データ処理者、管理者の役割を分離する；

④業務上、個人情報への一時的なアクセスを必要とする者に、一時的な権限を与え、その後、速やかに権限を撤回しなければならない。

個人情報へのアクセス管理の難点は、各権限管理者間の不適切なオフラインのコミュニケーションによる不正アクセスがないことを保証することである。アクセス過程では、従業員の役職から入手し、上位及び下位の役職間の各権限管理者の不適切なコミュニケーションをコントロールし、オンラインのアクセス権限と、オフラインの職務権限を統一的に管理する必要がある。

（5） 個人情報の管理

企業の管理層は、個人情報処理を監督する責任を担い、個人情報の分類、収集、保存、アクセスなどの処理を全面的に管理する必要がある。

管理層は、個人情報保護に関する法令の変更及び規制の動向に応じて、個人情報保護コンプライアンスマネジメントシステムを確立し、継続的に更新し、個人情報の取扱いに関する行動規範及び違反の結果を明確にし、外部コンプライアンス要件を社内規程に転換する。

具体的には、以下の措置を取ることが考えられる。

①社員教育の推進

個人情報取扱に関する社員教育・研修を定期的に実施することで、個人情報保護の重要性、自社のコンプライアンス方針及び関連管理措置、コンプライアンス責任、違反リスク等を明確にする。

②コンプライアンス体制の構築

個人情報保護のためのコンプライアンス体制を構築し、コンプライアンス文化を企業の生産および運営活動に浸透させる。コンプライアンス問題について全社員で意見交換できる仕組みを構築する；社会にコンプライアンスへの重視をアピールし、企業イメージを向上させる。

③リスクモニタリングの強化

人員、プロセスなどの安全要素から、リスクモニタリングを強化する。

人員面において、専門チームを編成し、専門人員によってリスク観測を行う。プロセス面において、実施可能かつ有効な管理プロセスを構築する。

④緊急対策の作成

個人情報セキュリティ問題の緊急対応メカニズムを作成し、実施する。是正措置を講じ、事件の影響と損害を評価し、さらなる影響を抑え、データとサービスの復旧に取り組む。

また、関連部門や個人にタイムリーに通知する。通知には、個人情報の漏えい、改ざん、紛失した情報の種類、理由と影響、是正措置、および危害軽減対策などを含める必要がある。

⑤定期的なコンプライアンス監査

企業は、定期的に個人情報取扱いの法律、行政法規の遵守状況についてコンプライアンス面の監査を行わなければならない。

コンプライアンスを遵守するには、定期的な内部監査または外部監査の実施が重要である。個人情報を取り扱う際、個人情報セキュリティにおいて、大きなリスクを抱えている企業は、外部監査を実施する必要がある。監査結果を踏まえ、管理体制の見直しを行う。

個人情報の管理は、個人情報取扱において最も重要な一環であり、個人情報の取扱全過程を監督・管理する必要がある。監督においては、具体の個人に責任を負わせ、各部門の責任者または中心メンバーが内部および外部の責任を負う体制にする必要がある。責任分担により、各部門の責任者が率先して個人情報保護の必要性やリスクを考慮したうえ、意思決定をし、監督と管理の役割を果たすことが可能となる。

6.『個人情報保護法』の限界

個人情報保護法には、法律の遅れやデータ開発の先駆けにより、必然的に限界がある。また、関連する司法解釈、法規制、およびその他の文書は発行されていないことのほか、以下の限界が見受けられる。

（1） データ管理のローカリゼーション

原則として、わが国の個人情報は国内でのみ保存および取扱う必要がある。個人情報を海外に送信する場合は、厳格なセキュリティ監査と評価を受ける必要がある。

個人情報のローカリゼーションはある程度のデータセキュリティを確保できるが、過度に厳格なローカリゼーションポリシーは多国籍企業の運営と管理に役立つどころか、成長を妨げることが考えられる。

（2） 個人情報取扱の集中管理の欠如

個人情報の管理は、主に行政機関によって行われ、各業界のデータ管理は業界ごとの主管機関によって行われる。しかしながら、データの越境流通における集中管理が欠如していること、また、法律面で、個人がクレームできるルートが設けられていないことなどが課題となっている。

7．予想される改正動向

現在、国内企業と多国籍企業の間には、個人情報に関する相互承認体制が確定されておらず、データの自由流通及び多国籍企業の業務展開の妨げとなっている。

社会のデータ化が進む中、国内企業は多国籍企業との個人情報共有を強化すべきである。中国は、他国と協力して、個人情報の越境流通を促進し、個人情報の相互承認体制の構築に力を入れるべきである。

8．終わりに

近年、新型コロナウィルスの影響による世界経済の停滞と保護主義的な貿易政策の台頭の中、経済のデータ化が加速している。企業にとって、データを利活用してビジネスに活かすことは今後の成長に必要不可欠である。企業は、法規定を遵守しながら、データのフル活用に注力すべきである。

『個人情報保護法』の施行により、IT 企業、多国籍企業の個人情報取扱活動に大きな影響を与えることは間違いない。一方で、新たな機会と挑戦を迎えることも期待されており、個人情報の管理能力は企業の新たなる核心的な競争力を構成する。個人情報の保護に積極的に取り組み、完全なるコンプライアンス体制を築き上げることは、企業にとって、競争優位性の構築に有利な影響を与えるだろう。近年、中国政府は、個人情報保護の監督管理を強化しており、長期的成長の観点からも、企業は自社の情報管理を徹底させるとともに、自らの情報管理体制を定期的に見直す必要があると言える。

（注）

(1) CNNIC が発表した「第 49 次中国インターネット発展状況統計報告」、http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202202/t20220225_71727.htm、2022 年 2 月 25 日

(2) PDA とは、「Personal Digital Assistant」の略語で、携帯情報端末のことである

(3) ビッグデータ殺熟とは、ビッグデータをもとに購入履歴や消費性向を分析し、新たにアクセスしてきた見込み客に安値を提示する反面、ヘビーユーザーや登録会員には同一商品に高額を支払わせることである。

(4)「個人情報保護法」73 条第 2 項により、自動意思決定とは、コンピュータープログラムが個人の行動習慣、趣味または経済、健康、信用などの状況を分析・評価し、かつ決定を行うことである。

(5)「個人情報保護法」45 条により、個人が指定の個人情報処理者への個人情報の移転を求め、国家網信部門の規定する条件に合致する場合、個人情報処理者は、移転ルートを提供しなければならないと規定している。

（参考文献）

(1) 王忠、ビッグデータ時代個人データプライバシー規制、pp.23（2020）、社会科学文献出版社

(2) 程嘯、個人情報保護法理解及び適用、pp.24～25（2021）、中国法制出版社

(3) 郭峰ほか、中華人民共和国個人情報保護法条文理解及び適用、pp.26～28（2022）、人民法院出版社

(4) 周漢華ほか、個人情報保護法条文精解および適用ガイドライン、pp.49～51（2022）、法律出版社

（原稿受領 2022.8.18）