PAUL HASTINGS

Stay Current

December 2020

Follow @Paul_Hastings

新型コロナニューノーマル下の業務上の行為義務と懈怠責任、推奨プラクティス
―日本の多国籍企業のためのグローバルな対応とリスク回避

By 新井敏之

I. ニューノーマル下の法的リスクとは

新型コロナウィルスの拡大が2月に始まって以来、それまで想定されてこなかった以下のような事象が頻繁に見られるようになった。これらの問題は各国法が個別に対応している最中であり、世界的なトレンドもできつつあるものの、いまだ解決模索中の段階といえ、世界中で営業する多国籍企業がどの法律を念頭に、どのような手法で、リスクを極小化するために対応すべきかというすぐれて実際的側面を含む。これらのリスクには、顧客、契約相手、従業員、規制官庁、競争相手などに関するものがある。ポイントは会社がリスクを回避し、極小化するためのなすべき義務を遺漏なく履践しているかであり、そうでない場合、過失や特別法で責任を問われたり、不利益を負うことになる。法的リスクには以下の例がある。

1. 自宅でコンピュータを使って勤務する、いわゆるテレワークの弱点に起因する秘密漏洩、ハッキング
2. 感染把握目的の使用に触発された個人の位置情報のeマーケティング目的での使用の日常化と位置情報の第三者との共有
3. コロナウィルスを口実とするフィッシングによる情報漏洩や、インストールされたランサムウェアを利用した情報の乗っ取り、その他のサイバー攻撃
4. ビデオ会議で営業秘密を議論することによる秘密性の消滅の懸念[1](消滅肯定例：デラウェア州のSmash Franchise Partners, LLC v. Kanda Holdings, Inc. No. 2020-0302-JTL, 2020 Del. Ch. LEXIS 263 (Ch. Aug. 13, 2020))

II. 問題意識

この状況を分析するにあたり、以下の問題意識を念頭に置く。

1. 日本の多国籍企業にとってこれらの事象に伴う法的責任の内容を理解し、対応するためには、どの国の法律をベンチマークに置くべきなのか
2. 不作為に関する過失の評価において、具体的に何をしないことが責任を惹起するのか、何をすれば免責されるのか、OFAC規制のように無過失責任である場合は、何をすれば責任軽減事由とされるか
3. ニューノーマル法的問題におけるハイリスク分野は何か、その場合の対応
4. 責任を負担するのは会社か、それとも取締役会や経営陣に属する個人も責任の対象となるか

III. リスクの検討

A. ベンチマークとなるモデル法の確定

日本の多国籍企業にとって本社は日本にあるから日本法を前提に行為すれば安全という訳ではもちろんない。そもそもニューノーマル下の法問題の範囲は広汎で、例えば以下の分野が関係している(本稿ではそのすべてには言及できない)。そのそれぞれについて、重大な結末はどの法律のもとで起きやすいのか、そして現実との兼ね合いでそれらについてどの程度準備しておくべきなのかを検討する必要がある。この作業の目的は行為義務違反(懈怠)に基づく責任を極小化するためである。

1. ニューノーマル業務形態下で会社の取るべき適切な行為義務とその懈怠から生じる過失(民事・刑事)
2. プライバシー・個人情報保護分野におけるプライバシーポリシーの内容、ベンダーなど情報共有者(例えば情報プロセッサー)との契約内容の確認・整備
3. 従業員のニューノーマル業務対応に関するEmployee Handbookなどの会社内部規則(会社の適切な行為義務の具体化について)の整備と実践
4. コロナを口実としたフィッシングから起きる情報漏洩対応や、OFAC規制でのランサムウェア支払のリスク(それ以外のリスクも存在)
5. HIPPA, 金融規制、消費者保護分野における個別の産業リスク
6. 経営陣、取締役の個人責任に関する会社法、その他の特別法の要件

これらのすべての法分野について統一的に単一のモデル法を想定するのは分野によっては現実的ではない。実際、多国籍企業が営業する世界の国々のどこかで問題を起こしたら、それは各別の対応を迫られる。しかし、だからと言って個別法にアドホックの対応をしていたのでは効率が悪いし、時宜を得た準備ができない。最大公約数的な対応を準備するのが便宜である。

したがって現実的なアプローチとしては、これらの法問題について新しい立法や判例の進展を示している、比較法的に先進的で、影響力のあるモデル法は何かと考え、そのうちでとりわけ重大な法的責任を課すものを一義的には世界オペレーションの基準とし、それとの距離関係を踏まえて各国の対応を微調整するということになる。具体的には現在、米国法がコロナ問題に最も迅速に適応しつつあると思われ、またエンフォースメントのモデルとしても重要である。米国は多くの企業にとっても最重要市場でもあろう。また個人情報の分野を除けばすべての分野にわたって対応の先鞭を示しつつある。但し米国法でさえも、すべての問題にタイムリーに十分な解決を示しえているわけではない。実態は現在正に法的な対応が議論され、実施されようとしている最中だということである。それ以外の国では先進的な対応を取る米国の対応を窺って、その概略が明らかになったところで類似の、しかし自国の事情を加味した対応を取ることになると予想される。日本もそのグループにいる。日本法がどのような対応を取るかは興味が尽きないが、それを待って対応したのでは多国籍企業の経営としてはリスクが高すぎる。

以下の検討は米法の現状を前提に記載される。

B. ニューノーマル業務下の会社の行為義務とその不作為による過失

1. 行為義務認定のファクター

民事にせよ刑事にせよ、その状況でするべきことをしないのが過失であるから、ニューノーマルという特異な文脈で業務遂行のために会社は何をすることを法的に義務付けられているかを検討する必要がある。

伝統的な法理論との関係でいえば、不法行為における保護範囲の決定(あるいは類似問題)と同様の方法で検討されると思われる。その場合、会社が置かれた具体的な事実状況において、①どのようなリスクが合理的に予想され、②それはどの程度の確率で生じると考えられ、③それから生じる損害の規模はどの程度のものであるか、及び④それを回避するために当事者に行為義務を要求することで生じる負担の程度、それらの相関関係を比較考量して具体的な行為義務が決定される。その義務を怠れば、該当国で過失に基づく損害賠償や個別法の罰則に服す

ることになる。さらに具体的には、⑤会社の規模、⑥業務分野、⑦業務の地理的範囲、⑧業務内容の複雑性、⑨競争業者の取る対応なども総合考慮される。また特別法で行為義務の内容の検討に追加要件が付されることもある。See, NY State Department of Financial Services' Guidance. [2]

2. ニューノーマル下の行為義務の具体例

(A) テレワークのリスク

ポイントは業務上のコミュニケーションがハッキングや秘密漏洩にさらされるリスクに適切に対応しているか。例えば、テレワークの技術要求が甘かった結果、顧客情報を流出させた場合などである。行為義務の検討で考量される要素は以下のようなものである。この問題については、同様の産業における、同様の規模の競争業者がどのように対応しているかがベンチマークになることが多い。その際の競争業者は国際的規模で想定される。その際、例えば日本で過失がないと認定されても、米国で過失があるとされることは可能である。その場合、より厳しい米国を念頭に対応する。

1. 業務用のコンピュータが各従業員に貸与されているか。
2. 個人用コンピュータを業務に用いることを許容している場合は、どのような利用の仕方をしているか(例・VPN, セキュリティソフトウェアの利用などがなされているか)。
3. コミュニケーションのためにエンドポイント同士で、VPNなどのセキュリティ対策が講じられているか。
4. サインインの要件は何か。パスワードの要件。
5. 二段階認証が要求されているか。
6. 個人用のメールアカウントの利用が制限されているか。
7. ヘルスケア、金融取引、ペイメント、消費者対応などの機微分野では、更に追加的な特段のセキュリティ対策が取られているか。
8. 上記事項の各々について、会社のEmployee Handbookはどのように規定しており、エンフォースされているか。
9. 会社のIT専門家が常時スタンバイしてセキュリティの問題に対応いるか。
10. テレワークのコンピューター使用について、会社としての訓練は行われているか。

これらのポイントのいずれかについて懸念がある場合は、リスクベースで重要性の原則にのっとり、優先度の高い対応をまずは行うべきである。その際には自分の会社と業種、規模の類似する会社の具体的な対応をベンチマークとする。

(B) 位置情報をめぐるプライバシー保護

ニューノーマル下ではマーケティング目的で個人の位置情報を積極的に利用するようになった。いまや携帯電話で使用される多くのアプリの目的の一つは位置情報の把握といってもよい。もはや会社にも行かないので、個人がどこで何をしているかは個別にでないと把握は難しいからである。さらに従業員の職務専念義務を査定するために位置情報を把握したいと考える使用者も多い。ただ位置情報は匿名化が難しく、個別情報である性質は容易に払拭できない。よってその機微性が大きい。したがって、問題が生じると深刻なものになりがちである。そのリスクには①データ主体からの請求と、②契約の相手からのインデムニティや債務不履行の請求がある。

この分野は行為義務の内容についても、まずは規制内容についてはGDPRを念頭に置きつつ、実務とエンフォースメントについては米法も念頭に置くという対応が好ましいと思われる。

何よりも、プライバシーポリシーで位置情報の利用について(そしてオプトイン、オプトアウトの選択について)具体的かつ詳細に利用者に開示し、それを遵守することはリスクを軽減する。基本的なポイントであるが、ニュ

ーノーマルの文脈でもう一度確認する価値がある。位置情報を利用する事業については、事業そのものの有用性と同程度に、プライバシー保護に遺漏がないかに検討すべきである（privacy by design.）このことは社員についての位置情報の把握についても基本的には同様であるが、よりプライバシーの配慮が必要だとも考えられている。

第三者の位置情報を入手する場合や、共同利用する場合の権利関係、とりわけコンプライアンスの表明保証や、インデムニティの十分性などの契約条件には注意が必要である。逆にこれらを要求される企業の立場からいえば、契約上のリスクをどう合理的にヘッジするかという問題がある。これらの現存する契約のディリジェンスを行うことが先決であるが、いずれにせよマーケット実務は依然流動的である。

また、国家レベルでの位置情報の利用を健康管理の見地から認める例があり、その場合の立法措置には様々なやり方がある。例・イスラエル、韓国。国家レベルの利用許容は特別の要件下で行われるものであるので、私人間の義務に影響を及ぼすものではないが、同様の態様でなされる私人間の権利義務の検討に参考となる(とりわけ機微情報の取扱い)。公衆の健康に関する開示である場合は、データ主体の同意がなくとも第三者に開示する道が開かれているのが通例である。例：日本の個人情報保護委員会、「新型コロナウィルス感染症の拡大防止を目的とした個人データの取り扱いについて」。もっとも、この方法は感染症対策とは関係のない位置情報には適用されない。

米国では第三者から取得する位置情報を冒用したとして、携帯電話会社にFCC の捜査が開始され、2億ドル以上の罰金が求刑されている例も発生している(Communications Act違反)ので、注意を要する。

(C)　従業員の義務：内部規則 (Employee Handbook)

ニューノーマル下のリスク対応として、従業員はどのような義務を負っているのか、何を会社は要求できるのかを明確にすること。内部規則に何も規定がないために、従業員がなすべきことをしなかったとしてもそれは会社の不作為の責任の問題とされがちである。反面、内部規則に規定があれば、それは従業員の個人的な義務違背ということで責任の程度に差があることは間違いない。例えばテレワークの方法の詳細が内部規則で記載されていた場合に、それでも情報漏洩があった場合を考えてみればよい。ポイントとしてはテレワークのリスク軽減策を成文化しているか、生産性の要求や報告義務等の手続きが可視化できているかが重要である。この点について実際的で有効な内部規則を整備し、それを実践することは過失の認定を妨げる事情となる。

作業としては会社がどのような行為義務が課されているかを上述した保護範囲設定の手順で検討し、そのうえで、それに対応する行為義務を従業員に課するという過程を取る。とりあえず上述のテレワークや手続要件違背等のリスクに対応するための内部規則を整備することが第一歩となる。ここでは世界市場での競争業者の対応状況を踏まえて、遅滞なく対応することが望まれる。

内部規則があっても、実際に履践されていなければ絵に描いた餅である。したがって有効性を確保する定期的な監査、訓練の実施は不可欠である。さらに国外の子会社関連会社について、これらの対応を行うことは親会社の法令遵守上の義務である。

IV. 暫定的なまとめ

行為義務の懈怠を回避するには、まずは正しい事実認識を念頭に、世界市場で一般に履践されている行為義務の実務を特定し、それを実行することが大切である。さらに特別法(成文法、判例)の発展に注意を払い、それに対応する必要がある。

ニューノーマル下の行為義務違反が紛争になるのは、大きな損害が発生する場合か広範囲で違反が暴露する場合であると考えられる。その意味で行為義務の検討にはリスクベースで対応することが必要である。本稿では触れるいとまがなかったが、ハイリスクとされる産業と業務内容が存在することは知られており、とりあえず金融、ペイメント、ヘルスケアなど、中でもBtoCの分野で注意を払うこと(一般の行為義務よりも厳格な行為義務の措定)が必要である。経営陣や取締役の個人責任を追及する請求原因も多い(一般法、特別法ともに)。さらに、リスク対応の目的は損害を実質的に回避することであり、形式的なウィンドードレッシングすることに意味があるのではないことに注意すべきである。

以上

✧ ✧ ✧

本稿の内容についてご質問等がございましたら、担当者までお気軽にお問い合わせください

Tokyo

新井敏之
81.3.6229.6010
toshiyukiarai@paulhastings.com

---

1 経産省「テレワーク時における秘密情報管理のポイント」(5月7日)も参照のこと。

2 Shirin Emami, *Re: Guidance to New York State Regulated Institutions and Request for Assurance of Operational Preparedness Relating to the Outbreak of the Novel*, March 10, 2020, https://www.dfs.ny.gov/industry_guidance/industry_letters/il20200310_risk_coronavirus, last visited Nov. 27, 2020