技術の向上とサイバー詐欺の変容

――AI 技術の発展と刑法の課題に関する一考察――

韓　草

目　次

はじめに

情報技術が発展するにつれ、インターネットは人々の日常生活の第二空間になった。これは、ソーシャルネットワークとも言われている。そして、現実社会とソーシャルネットワークが、相当程度融合している。ソーシャルネットワークには、巨大な財産も集積しており、そうであるがゆえに、ソーシャルネットワークはまったく新しい犯罪領域になった。

サイバー犯罪も多様であるが、そのうちの典型的なものの 1 つが、サイバー利用詐欺である。行為者が、ネットワークを犯罪のプラットフォームとして利用し、虚報の情報を発信して、他人の財産を騙取する、というものである。表面的に見れば、これと伝統的な詐欺罪とは刑法解釈上は同一である。伝統的な詐欺罪における行為者も、不法占有の目的をもって、虚偽を述べて他人を錯誤に陥れ、財物を騙取する。しかし、伝統的な詐欺罪に一般的な、人と人とが対面して行われるような態様とは異なり、ネットワークのプラットフォームには、

拡散性や即時性などの特徴があることから、サイバー詐欺罪の有する社会的な危害性の深刻さは、伝統的詐欺罪とは異なる。

さらに、科学技術の発展に伴い、科学技術自体も、サイバー詐欺に一定のチャンスと挑戦とをもたらした。現在高度に発展している人工知能（Artificial Intelligence、以下では「AI」という）技術はビッグデータ収集分析を支えている。これはサイバー詐欺の展開とある程度一致している。AI は私たちの生活に関係しているが、例えば、日常的に使われている指紋認識、顔認識、スマート検索などの技法は、サイバー詐欺でも利用可能なものである。

これに対し、一部の機関や企業はビッグデータ分析、機械学習などの AI 技術を積極的に利用して詐欺の防止や管理をするようになり、それに対抗する詐欺犯も、AI を積極的に利用して詐欺を実施し、詐欺はコストが低くなる、態様が多くなる、波及効果が広くなるなどの特徴がみられるようになっている。「インターネット +AI」時代の進展に伴い、これらの状況はより多くかつ複雑になり、これは法律上にも一定の影響を与えると思われる。新しい時代には、新しい一連の問題がもたらされるのであり、法律にとって、それへの対応をし、それを完備させる必要があるといえよう。刑法は、時代の変化に敏感に対応しなければならない[1)]。

これらの状況に対して、本稿では、AI がサイバー詐欺に与える影響と対応について検討することにしたい。

なお、本稿では、サイバー詐欺とは、インターネットのネットワークを利用した詐欺、AI 詐欺とは、詐欺のスキームのいずれかにおいて AI を利用する詐欺を指すものとして定義する。また、AI についても明確な法的定義などはないのが現状であり、例えば、「人工的に造られた、知能を持つ実体」とする定義もあるが、本稿では、『東京都 ICT 戦略』（2017 年）などが採用している「人間の脳が行っている知的な作業をコンピュータで模倣したソフトウェアや

1） 李振林：《人工智能刑事立法图景》、《华南师范大学学报（社会科学版）》2018 年第 6 期。

システム」[2]といった意味で用いることにする。

一、問題意識

1. 中国初の AI サイバー詐欺事件

2017 年 9 月、中国の浙江省紹興市で、警察は中国初の AI を利用した詐欺事件を摘発した[3]。事案の概要は、以下のとおりである。

2017 年 1 月、紹興市民の虞某は親友からの代理支払い請求に関する情報を受け取り、ネットリンクで“友達”を助けて 1000 元余りを支払った。ところがその後、親友のネットアカウントが盗まれていたことを知り、虞氏は騙されたことに気づき、公安局に通報した。

虞氏が騙された事件を契機として捜査に着手した警察は、手がかりを詳しく調査し、ハッカー技術を利用した違法なインターネット上の「黒色産業チェーン」（“black industry chain”）の全体像を認知するに至った。そこでは、犯罪者は、ハッカー技術を利用して、ウェブサイトのバックグラウンドユーザー登録データ、データ衝突ライブラリ（Data Credential Stuffing）を不正に取得し、インターネット会社のセキュリティ対策を迂回するなどの手段を用いてサイバー詐欺、不正情報普及等を行っていた。この事件の進行過程において、ハッカーの楊氏が構築した“快啊”というコードプラットフォームが、AI 機器のディープラーニング方法を用いて機器を訓練させ、画像検証コードを自動的かつ迅速に識別することができるようにしていた。そうすることで、ネットワークサービス提供者が設定したアカウントの安全なログイン保護を、容易にバイパスすることができるようになった。この“快啊”というコードプラットフォー

2）　東京都『東京都 ICT 戦略』（2017 年）48 頁。

3）　人民網による報道。その概要は　http://zj.people.com.cn/n2/2017/0923/c186938-30767452.html（2020 年 9 月 4 日閲覧）（刘宪权　房慧颖《涉人工智能犯罪的类型及刑法应对策略》、《上海法学研究》集刊(2019 年第 3 卷　总第 3 卷）において引用されている）

ムを使って、黄某らの犯罪グループはサイトの脆弱性を利用してネット情報システムに不正に侵入し、Web バックグラウンドユーザーの登録情報を取得し、10 万組のデータを 1 単位として、ライブラリソフトウェア（Credential Stuffing software）を作成するグループに販売した。呉某、魏某などの衝突ライブラリ（Credential Stuffing）の担当用員は、データを取得した後、直接“快啊”コードプラットフォームとドッキングして大量の衝突ライブラリのマッチングを行い、各種類の口座をパスワード照合に成功した口座情報を再梱包してネット詐欺グループに売っていた。最後に、鄭某を代表とする詐欺グループが、不正取得したデータを利用して様々な詐欺活動を実施していた。

2. ヨーロッパ初の AI サイバー詐欺事件

イギリスのデイリーメール（Daily Mail）紙の 2019 年 9 月 6 日付報道によると、同年 3 月、ある詐欺師が、AI 音声模倣ソフトを利用して会社の大ボスになりすまし、イギリスのエネルギー会社の CEO にドイツの親会社のボスと電話していると信じさせることに成功した。電話中、詐欺犯は、この CEO に直ちに 22 万ユーロをハンガリーのサプライヤーの銀行口座に振り向けるよう要求し、“滞納金”の納付を避け、振込情報をメールで送信するよう求めたが、ドイツの親会社のボスであると思い込んでいたため、この CEO は迷わずそうした。結局この金は二度と戻ってこなかった。これは、ヨーロッパで初めて報道されたサイバー詐欺事件である[4)]。

アメリカのワシントン・ポスト紙（The Washington Post）によると、この CEO は後に電子メールで、この要求はかなり“おかしい”と指摘したが、“大ボス”のドイツ語なまりの英語は非常にリアルで、自分は服従するしかないと思っていた。詐欺犯が使っていたある人工知能ソフトは、他人の声やイントネーションを真似するだけでなく、ドイツ語なまりの英語も真似することができ

4） 人民日報海外網による報道。その概要は https://baijiahao.baidu.com/s?id=1644099490138679040&wfr=spider&for=pc（2020 年 9 月 4 日閲覧）

るものであった。この CEO は当時、ドイツのオーナーと話していると思っていたので、会社が罰金を延滞しないよう、その支援のため、要求通りに 1 時間以内にこの金員を送金した。

詐欺犯は、被害者であるこの CEO と全部で 3 回電話で会話をした。2 回目の電話は、22 万ユーロを送金した後であり、相手はこの CEO に電話をして、親会社がイギリス会社の費用を返済するために資金を移していると伝えた。その日の夜、この CEO が 3 回目の電話を受け、当該詐欺師がドイツのボスになりすまして 2 回目の支払いを要求したとき、彼は何かがおかしいことに気づいた。相手が約束した振込返済資金が届いていない上に、3 回目の電話番号は発信元がオーストリアであることを示しており、疑念を抱いたところから 2 回目の金員を支払うことを止め、ドイツのオーナー本人に直接電話したところ、騙されていたことが分かった、という事案である。

3. 検討

AI が世に登場し、すべての人が AI の能力に驚き、誰もが AI の技術的進展の方向を見極めたいと興味を持っている。たとえば“AI 音声合成”について関連するニュースも多くの人が接したはずであり、“チャットアプリから著名人の声真似機能が発売される”、“AI だけであなたの発話を模倣できる”など、技術への楽観的な期待を伴い、関連技術成果も研究者によってオープンソースプラットフォーム上でひろく共有されている。この他にも、様々な顔加工アプリなども次々と登場し、私たちはその楽しさを享受している。こういったすばらしい状況の中で、今般の“AI 音声詐欺”事件は、まさに私たちの目を覚まさせるものとなった。

数年前に頻発していた、携帯電話事業者になりすましたメール詐欺も、ここ 2 年ほどの“お茶売り”WeChat 詐欺も、“裁判所からです”、“警察署からです”という公検法（公安・検察・法院〔裁判所〕）になりすました電話詐欺の存在や手口も、すでにネット上で明らかにされており、騙される人も減少してきてはいる。しかし、詐欺師はこのまま姿を消すはずはない。AI 技術が発展して

おり、また、技術の成熟に伴い、応用のためのハードルも低下しており、人工知能が簡単に入手できる携帯アプリになるほどにまで、一般人も簡単に利用できるようになっている。“気の利く”詐欺師が、詐欺の方法を“AI 化”しているのである。

犯罪者は、最低限のコストで目的を達成できるツールを利用する。普通の人はまだ AI がよくわからない状況ではあるが、詐欺師は、AI を使って詐欺ができるようようになった。このような詐欺事件は珍しくない。人民日報のインターネット版である人民網も、WeChat で友達や家族の助けを求める声を聞かされて騙された事件を報道したことがある。音声チャット、ビデオ通話など、古いように見える品のない詐欺術は、なぜ AI の技術を使うと、いとも簡単に人間をだますことができるのだろうか？　現在の技術では、アルゴリズムによって人間の全セットの音声を生成することができ、異なる口調でも本当のそれであるかのようになっている。音声詐欺は、AI 詐欺の一角を明らかにした。人々が、以前の古い詐欺術が意にかけるには及ばないと油断している間に、詐欺師は、すでに AI という新技術に熟練し、巧みに利用しているのである――そのアルゴリズムは、騙されたグループを選別し、当該個人の特徴と好みを分析して、ロボットは定時に嫌がらせ電話をかけて、それに顔を加工し、声を変えるなどの一連の操作を加えて、そういった加工がなされていることを信じさせ難いようになっているようにも思われる。初の AI 詐欺が発生してからしばらくが経過しているが、ますます簡単で使いやすいオープンソースの顔・音声加工アプリが登場するにつれ、AI 詐欺のコストはますます低くなっている。それと伴に、それによる新たな詐欺方式は、当局による対応も十分できないだけでなく、ますます頻繁に発生し、「狂気じみて」すらいる。

このような状況の下、一般人は、AI 詐欺に対してどのように対応すればよいのだろうか。AI が詐欺に使われた時、その責任は誰に帰属させるべきなのか。新たな法律が必要となるのか、あるいは現行法に基づいて何らかの対応をすればよいのだろうか。より深く考えて、AI が人間のように独立して思考と意思決定をすることができ、人間の代わりにある仕事に従事し、ある役割（例えば

自動車運転）を担当することができるような場合、AI の権利と義務はどこに求められ、法律は、どのようにその中での複雑な関係を調整することになるのだろうか。AI が犯罪事件にかかわる時、責任主体はどのように定義されるのか、AI は、法律と道徳意識と行為能力を持つ主体になりうるのだろうか。もしそうでなければ、いったい研究開発者、運営者、それとも利用者が責任を負うべきなのだろうか。逆に、もし AI が行為能力のある主体であることを認めるとするならば、“容疑者 AI”は、どのように有罪判決を受けるべきなのだろうか。

これらの問題は、すべて私たちが深く考える価値があるといえよう。

二、サイバー詐欺への AI の応用

1. AI 利用サイバー詐欺のよくあるタイプ

AI 利用サイバー詐欺の事件は多数生じているが、その手口は、実はほぼ同じである。現在よく見られる Al 詐欺には以下のような類型がある。

A. 第一類型、メールや署名などの偽造

署名を偽造するというタイプの詐欺は非常に古いものである一方、もともとはめったに生ずることはなかった。しかし現在では、Al 技術との結合により、再び注目を集めている。

2017 年、アメリカの南オレゴン大学（Southern Oregon University, SOU）は騙されて、190 万ドルの送金を行った。大学は、自らの振込対象は学生娯楽センターの建設を担当するアンダーソン建設会社だと思っていたが、実際には、詐欺犯の銀行口座に振り込まれた[5)]。詐欺犯は、既定の建設会社になりすまして学校財務部門に支払請求書を送付し、それを信じた大学が、その後に金員を詐欺師の銀行口座に送金した。この事案では、大学を錯誤に陥りやすくさせ、メールの内容を信じさせてしまうことに、AI が大きな役割を果たしている。

5)　事件は安全牛網より《BEC 攻撃再現：大学からメールで 190 万ドルをだまし取った》https://www.aqniu.com/news-views/25999.html（2020 年 9 月 4 日閲覧）

このようなビジネスメール詐欺（Business Email Compromise, BEC）なら、攻撃者は Twitter、Line、Facebook などのソーシャルメディアにより、詐欺の対象者の業務に関する情報は簡単に得ることができ、企業や機関の公式サイトでも、自らの組織機関や管理者を公開しているため、年齢、性別などの多次元データは機械学習訓練モデルに投入することができる。例えば、会社の管理者が Twitter で自らのスケジュールを公開しているという場合、機械学習訓練モデルのシステムはいつ会議に参加しているのか、仕事をしているのかを見分けることで、攻撃戦略を調整し、AI 言語モデルを介して一貫した納得できる内容のメールを生成することができる。よくあるのは、支払い口座の変更や緊急支払いを要求することであるが、役員が休暇や長距離飛行中に、従業員らが本人に連絡することは難しく、無防備な被害者として、“緊急事態”であることから、号令に従うことを選択しがちとなる。

この方法は単純にすぎるように見えるが、しかし、連邦捜査局（FBI）のデータによると、FBI は 2019 年に 467,361 件のサイバー犯罪の報告を受け取り、機関はこれらの報告における損失が 35 億ドルを超えると推計している。この損失のほぼ半分は、BEC に由来するものである[6)]。最も重要なのは、フィッシングページやファイルが存しないため、このような欺罔行為をセキュリティソフトウェアで選別することは困難であり、アドレスも内容も“合法である”ように見えることである。

警戒を高め、慎重にチェックすれば、メール詐欺を高い確率で防ぐことができるとしても、AI が筆跡を偽造するといったような個性的な特徴の欺きは、本人をよく知っている友人でさえだまされやすくなるかもしれない。イギリスのユニバーシティ・カレッジ・ロンドン（University College London, UCL・ロンドン大学）の研究者は、“My text in your hand writing”という AI アルゴリズムを開発した。これは、1 人の字形とその特殊な書き方を分析し、字形、サ

6） データは cnBeta より《FBI の報告書によると 2019 年の BEC 詐欺はサイバー犯罪の損失の半分を占めている》。

イズ、色、筆線テクスチャ、垂直および水平間隔などまったく同じ筆跡を生成することができる。これまでで、人間の筆跡に対する最も正確な複製である。現在では、中国でも日本でも、本人の署名が必要な場合が多い。例えば、借用書がそうである。もちろん、借用書は軽微なケースにすぎず、おそらく犯罪者も、労力を簡単にしかかけず、一人だけでは騙されないだろう。しかし、より高い精度を持つ法律文書や金融文書、例えば財務契約署名、遺言、歴史的人物の手跡などを偽造すれば、司法証拠の鑑定と不正証拠の排除に多くの困難をもたらし、事実の鍵となる方向を変える可能性がある。さらに、AI 生成アルゴリズム能力の向上に伴い、将来的には、専門鑑定士が筆跡の真偽を識別することは容易ではなくなるだろうともされている。

B. 第二類型、AI による音声合成や顔の加工

メールも手書き文書も、現代人の生活様式のなかでは、その意義は薄れてきている。しかし、上記の詐欺方式が対策が講じられていないうちに、より判別しにくい新たな手段が現れた。これが最近大ヒットした AI の変声と顔加工である。

2017 年に Deepfake が登場してから、AI が顔を加工するという事象が人々の視野に現れはじめ、そしてより操作が容易な Fakeapp が登場し、一般人も顔を加工する技術が使えるようになった。様々な顔を変えたり、声を変えたりするアプリは、AI 技術に基づくアプリケーションがネット上でブレイクし、各アプリケーションショップで盛んに展開されている。“顔を変えて声を変える”ことが流行している。ネット上には様々な芸能スターや政府要人の顔加工動画が登場しはじめた。禁止されているところはたくさんあるが、効果は理想的ではないようである。

現在では、ZAO の登場が、AI 顔交換技術の議論ブームに再び火をつけた。ZAO に写真をアップロードするだけで、ビデオ P を対応する顔にすることができ、操作が簡単で効果的であるといえる。そこで各サイトには猥褻動画を流したサイトも含めて AI が顔を加工する動画が大量に登場し始めた。アリババの運営するオンラインモールである淘宝網でも、AI 顔交換サービスを購入す

ることができる。現在の AI 顔交換技術は驚くべき水準に達しているが、現在の多くの AI 顔交換技術は視覚にしか触れていない。

しかし事態は変化している――AI が顔を加工することが現実になっており、AI の変声も現れ始めている。AI 変声技術は成熟してきており、AI 顔交換技術と組み合わせると、威力がより強くなる。以前、AI によって顔を加工したり、AI によって声を変えたりして、偽のオバマ演説ビデオが偽造されていることがあった。動画では、オバマ氏がトランプ氏を“バカ”と非難しており、驚きに値するものであった。この動画は海外でセンセーションを巻き起こしており、特に表示されていなければ、本当だと信じている人も多いだろう。ますます多くの、スターや政府要人が声を変え顔を変えた上での悪しきビデオがネット上で伝わるようになり、人々は最初は現在の科学技術の発展に驚きと好奇心に驚いただけでなく、AI が顔を変えて声を変えることによるリスクを考えるようになった。

まず、このような状況では、情報の真実性が懸念される。PS 発明後、真実はない図画があり、AI ビデオの顔変換技術が登場すると、ビデオも同一の状況になった。もともと偽のニュースが飛び交うインターネット上では、さらなる信頼の崩壊につながることは間違いない。さらに、これは肖像権を侵害する可能性を大幅に増加させるだろう。誰もが、自分の顔がわけのわからない動画に出てくることを望んでいない。

もちろん、この AI 技術はもともと賢い詐欺師にとっては完璧なツールである。人々は、借金をした人が、本当に自分の家族と友達なのかどうか、もっと分かりにくくなるのではないか。中国の人民網では、趙氏が父親からの Wechat のメッセージを受け取り、自分が野菜を買ってお金を持っていないと申し述べていたため、200 元を送金させたという事案が報じられたことがある。趙氏は疑問に思って、“お父さん、あなたはお父さんですか？”と尋ねた。“父”であるとの言葉を受け取ると、趙氏はお金を振り込んだ。しかし、この父親の言葉は、詐欺犯が AI で声を変えて合成したものであり、本当の父親から来たものではないとは誰も予想し得なかった。例えば、映像と音声とを結合して加

工させたのであれば、音声確認後にもう一度ビデオで確認しても、完全には確定できないかもしれないと考えられる。現在、この点で判決の下された事件はまだ存在していないが、これは、懸念されることであると言わざるを得ない。

C．第三類型　AI 技術により、被欺罔者の選別、被欺罔者のチャット習慣、生活特性などの情報の取得。

上記の 2 つは、被害者の家族や友人になりすましているのとは異なり、AI 技術により被欺罔者を選別し、被欺罔者のチャット習慣、生活特性などの情報を取得した後、被害者と連絡を取り、被害者の信頼と共感とを得るタイプのものである。人をだますのに適した好みや習慣に合わせて、計画的に被害者らと付き合い、少しずつ財物をだまし取るのである。

2017 年 12 月、中国・広東市は、中国初の交友 APP 新型ネット詐欺事件を摘発し、処罰した。これは、出会い系携帯アプリでチャットしている“キャスター”に“ロボット”でなりすまし、プレゼントを請求することで詐欺を行うものであった。

2017 年 8 月、広東省公安庁網警総隊は、珠海警察に通報し、ネット上に“某城求愛”という携帯アプリがあり、交友、求愛を看板に、まず隠された宣伝方式で男性ユーザー登録会員を誘致し、様々な消費方式を設けてユーザーに大量に資金投入させてネット詐欺を実行していることを通告した。“某城求愛”携帯電話 APP は 1 種の新型のネット詐欺事件であり、この犯罪グループは、あるネット有限会社を主として、完全な会社運営を行っていた。また、各主流サイトでは、“同じ地域に居住”“求愛”“結婚”などの敏感な言葉や、“露出写真”が注目され、ユーザーがこのアプリをクリックしてダウンロードしていた。ダウンロードすると、同プラットフォームの女性“キャスター”が自発的にユーザーに声をかけるが、実際には、この犯人グループがコードを用いて“ロボット”プログラムを作成して女性ユーザーになりすまし、あらかじめ設計されたモデルに従って自動的に男性ユーザーに“挨拶”を送信する。そして、相手と話し続けるためには 200 元かけて VIP 会員に登録しなければならず、登録が成功した後に相手とビデオを送りたい場合は、ビデオタイムに応じて料金を

請求し、“プレゼント”などと呼ばれ、不正に利益を貪る必要がある。一方、携帯電話画面の反対側でユーザとチャットしている多くは、実際の登録ユーザではなく、ユーザをだまして消費をさせ、交友、結婚恋愛などの目的はかまわないのが実態であった。

統計によると、バックグラウンドだけを管理して調べることができる 2016 年 8 月から現在までのチャージ金額は 3.4 億元に達し、毎日 30 万元ずつ増加し、同時に同社が作成した 127 個の“ロボット”プログラムの 1 日の“収益”は 4 万元を超え、だまされた人数はすでに 100 万人に達している。(以上の金額は全部人民元である。)

悲しいことに、昔は少なくとも被害者を騙したのは人であったが、現在はただの AI である。騙すメカニズムは、実は従来のネット詐欺に比べてあまり目新しいところはないが、AI が結合することで詐欺過程に要するコストが安くなり、結果的に実現しやすく、威力も強くなるのである。

2. サイバー詐欺への AI の積極的な影響

以上では、技術の高度化が詐欺類型に与える影響を、詐欺犯の観点からみてきた。これに対して、ビッグデータ分析(Big Data Analysis)、ナレッジグラフ(Knowledge Graph)技術などの技術が応用されるに伴い、詐欺防止のための管理にも、大きな便宜をもたらした。

ビッグデータ解析に基づくサイバー詐欺防止管理技術の応用は、データマイニング分析結果を基礎とし、全体の過程は“データ収集、データ処理、データマイニング”などの多数のコースを含む[7]。データ収集と処理レベルでは、主に企業独自システムで取得したデータ、インターネットで採取したデータ、第三者から購入したデータの 3 種類のデータソースがある。これらのデータはスマート化処理を経て、その後にデータ分析と発掘とを展開し、サイバー詐欺行

7) 中国信息通信研究院安全研究所 2019 年 12 月《电信网络诈骗治理与人工智能应用白皮书(2019 年)》第 3 页

為を識別し、完備した技術防止システムを構築するためにデータ基礎を構築する。データマイニングレベルでは、ビッグデータのマイニング能力を利用して、詐欺行為の典型的な規則を発見することができ、詐欺犯と詐欺行為を正確に識別し、さらにサイバー詐欺に対して正確な警報を行うことができる。

ナレッジグラフ技術は、図に基づくデータ構造であり、データから作成された 1 枚の知識図と見なすことができる。予防管理への応用において、ナレッジグラフ技術は、多種のデータソースを関連させることができ、モニタリング目標分析に対してその脈絡、傾向および特徴を識別し、重要な詐欺情報検索、アカウント関与リスク評価、詐欺グループの判断、異常行為分析など大きな役割を果たす。

これらの AI 技術を利用して、あらゆる条件下での詐欺電話の測定を行い、大量の通信データに対して前処理を行い、分析、比較とモード識別を行うことができる。詐欺重点区域のローミング動態モニタリング、データ分析、そして迅速なハイリスク関連詐欺番号の処置が実現される。その他、データサンプルライブラリに基づいて、大量のサイトに対して特徴検査、ページ類似度分析を行うよりも、ブロック疑似詐欺サイトを迅速に発見することができる。既知の詐欺情報を絶えず学習することによって、相応の処理処理を結合し、リアルタイムで情報の信頼性を分析し、判断することができ、恐喝あるいは偽造内容を早期に識別することができる。さらに自動架電（パソコン用電話ソフトで自動的に電話をかけること）、警報メッセージの送信などで被害が疑われる利用者に速やかに注意する。例えば、アリババの銭盾反詐欺公益プラットフォームは反復警報モデルを絶えず更新し、自動化された詐欺行為と被害を受けたユーザーの適時発見警報能力を形成する [8)]。

2016 年 12 月に、中国の W 省公安機関と W 省通信管理局は協力して“全省通信ネットワーク遮断システム”を構築した。その作用原理は、詐欺犯罪者と

8)　魏薇、尚鉄力、周帥《人工智能対电信网络诈骗治理的影响及应对思路》《信息通信技术和政策》2020 年第 4 期 第 81 页

詐欺の被欺罔者の規則性の分析、精緻化を通じて、異常行為動態分析ビッグデータモデルを構築し、能動的にデータ分析研究判決を展開し、そして研判結果を電気通信部門を通じてだまされやすい人たちに送って、サイバー詐欺犯罪に打撃と防止を行うというものである。この通信ネットワーク遮断システムは、2016 年 12 月から利用されている。これにより、第 1 期の完成効果は非常に明らかであり、すでに公安部の普及サンプルになっている[9]。これらの AI 技術により、警察など法執行機関が、大量のデジタルデータ等をコンピューター上で分析し、その結果に基づき、被疑者の特定等の犯罪捜査、または犯罪予測に基づく警備活動等を行うものである。それによって警察活動の精度の向上や効率化が図られている。

もし、ビッグデータに基づく AI 解析や犯罪者のプロファイリング（profiling・推測に基づく犯人像の分析等）によって、より正確な情報に基づく合理的な嫌疑を認識できるのであれば、警察としても、当該犯罪等と無関係な第三者を巻き込むことなく、実際の犯人等を、より的確に対象とした法執行が可能になると言える[10]。

3. サイバー詐欺への AI の消極的な影響

以上で検討してきたように、AI 技術は、詐欺防止にも使えるし、同様に詐欺行為にも使える。これも先に述べたように、AI 技術は、従来のサイバー詐欺の 4 つの段階で利用でき、詐欺をより容易にして、発生する損失額も多額のものとなる。そのため、サイバー詐欺への対応が厳しくなっているが、この類型の事件が年を追って増加している理由として、AI による幇助が、その一つの要因であると考えることができる。

---

9) 马忠红《以电信诈骗为代表的新型网络犯罪侦查难点及对策研究——基于Ｗ省的调研情况》《中国人民公安大学学报（社会科学版）》2018 年 3 期 第 84 页

10) 星周一郎「ビッグデータ・ポリシングは、今後の社会に何をもたらすか？ ―ICT・AI 技術を活用した警察活動に関する議論の展開に向けて―」都法 59 巻 2 号（2019 年 1 月）

一般的に、サイバー詐欺には“正確な情報取得”、“詐欺スクリプト設計”、“通信連絡誘導”、“資金支払い移転”の 4 つの場面がある[11]。従来のネットワーク詐欺、電気通信利用詐欺に対して、AI 詐欺の状況には目新しい点は存在しない。AI 詐欺とは、AI 技術が犯罪者によって詐欺を実施する各段階に用いられることである。具体的には以下の図 1 に示すとおりである。

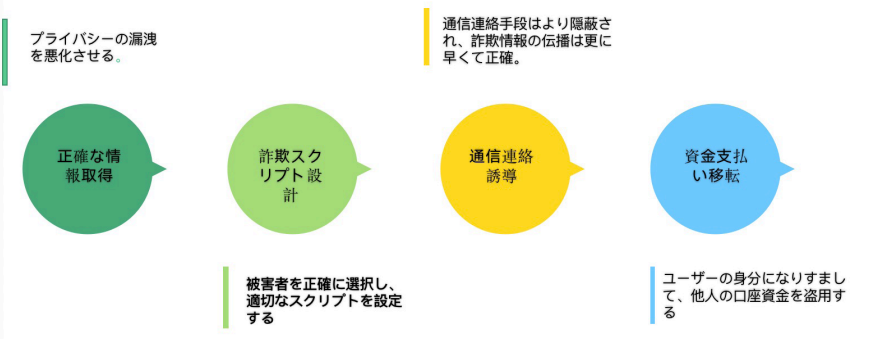

図 1

図 1 の通り、“正確な情報取得”の段階では、AI 技術でネットワーク攻撃によりシステムを破壊し、データを盗取しやすくし、大量のユーザの個人情報などを得ることができる。また、個人情報を取得する経路はより多様化し、方法はより隠密的な形で、個人の重要な情報を正確に抽出する。従来のサイバー詐欺よりも、プライバシー情報の漏洩が悪化させられていると認められる。“詐欺スクリプト設計”の段階では、AI 技術は、人を正確に模倣することができるようになった。大量のデータ入力とディープラーニングを経て、AI は一人の人間の好み、状態を正確に判断することができる。そして、詐欺犯は、AI 技術で特定の人々の行動特徴を訓練学習することにより、様々な特定の詐欺シナリオを作成する。なお、詐欺犯も、AI 技術で取得したデータにより、被害者を正確に選択して、たとえば、感情利用詐欺を実施する場合には、感情に関

11）　中国信息通信研究院安全研究所　2019 年 12 月《电信网络诈骗治理与人工智能应用白皮书（2019 年）》第 10 页

する情報を常に発信している人を選別することができ、金融詐欺を実施する場合には、常に投資情報を収集している人を選別することができる。“通信連絡誘導”の段階では、通信連絡手段はより隠匿され、詐欺情報の伝播はさらに早くて正確である。例えば、ロボットが詐欺電話をかけるとすれば、「人による電話」では、人間一人当たり毎日 300-500 件の電話をかけることができるが、1 つの架電ロボットは、毎日最大 5000 件の電話をかけることができ、人力コストは 80% 低下し、効率は 200% 向上することになり、人手コストは大きく削減される[12)]。あるいは、最初に紹介した 2 つの事件のように、AI 技術を利用して音声合成を行い、顔を変えて声を変えることで、怒りや喜びなどの異なるニュアンスの感情までこなすことができ、偽造された音声やビデオで被害者に連絡し、信頼性が高く、騙される可能性がより高くなる。

最後の“資金支払い移転”の段階では、中国では、現在は、基本的に現金を持つ必要がなく、携帯電話での支払いが著しく普及しており、また利便性も高い。しかし、このような知能化は、新たなリスクをもたらした。人工知能の応用は、大量のデータを収集・処理しており、攻撃されると、ユーザのプライバシー情報が暴露されやすい。さらに、AI 技術によりユーザの顔の特徴を取得し、指紋などの生体特徴によって、ユーザの身分のなりすまし、他人のアカウントの盗用といったリスクもある。

そのため、行為者は、AI を利用する詐欺犯罪は、手段がさらに隠匿的なものとされ、犯罪効率がより高まり、伝統的な詐欺と比べて、さらに大きな利益をもたらし、それによって、詐欺師にとってはさらに“冒険”するに値するものとなる。しかし、AI の法律性質などの根本的な理論上の問題についてはいまだ共通認識に達しておらず、刑法は現在、立法の上で、このような新型詐欺犯罪を明確に規定することができず、司法実務において、このような行為に対する性質の評価はまったく統一されていない。

12) 中国信息通信研究院安全研究所 2019 年 12 月《电信网络诈骗治理与人工智能应用白皮书（2019 年）》第 13 页

そのため、このような問題は、なお検討する必要があると考える。

三、AI がサイバー詐欺にもたらす問題と対応

1．問題

科学技術レベルの向上に伴い、AI の発展も日進月歩である。人工知能の発展を段階的に分類すると、人工知能を弱い人工知能（Weak Artificia Intelligence）、強い人工知能（Strong Artificial Intelligence）、およびスーパー人工知能（Super Artificial Intelligence）の 3 種類に分類することができる[13]。AI の商業、交通、医療、教育などの社会各分野での広範な応用に伴い、これらをきわめて便利なものとするのと同時に、技術発展に基づく固有のリスクが、いくつかの法的な認定を必要とする問題をももたらした。

当然のことながら、刑法は時代の変化に敏感に対応しなければならない[14]。新しい時代は、新しい一連の問題をもたらすのであるから、我々の法律も、それへの対応と完備を目指す必要があると思われる。

㈠、AI の刑事責任の認定

自動運転車による交通事故について、自動運転車そのものの刑事責任を追及できるかどうかから、工業生産における知能ロボットが惹起する人身傷害行為において、刑事責任主体となりうるかどうかの根拠、さらには、インターネット検索エンジンを介して編成された侮辱的な語彙が、知能ロボットに対して侮辱、誹謗罪を成立させることができるかどうかなどに至るまで、中国の刑事法の分野では、人工知能の刑事主体としての地位を検討する議論が盛んに展開されている。主として、人工知能（ロボット）が刑事法的責任主体となるかどうか、法益侵害結果が発生した場合に人工知能に単独で刑罰措置を加えることができるかどうかなどの問題に関心が集まっている。

13）　刘宪权《人工智能时代的“内忧”“外患”与刑事责任》《东方法学》2018 年第 1 期第 135 页

14）　李振林・前掲注（1）論文。

ある学者は、人工知能時代の刑法整備において、人工知能ロボットに刑事責任主体の地位を与えることを適時に考慮すべきであると考えている。根源からリスクを防止し、人工知能乱用罪を新設する、あるいは、厳格な責任を確立し、人工知能事故罪を新設するといったことを提案する[15]。また、別の学者は、現在の人工知能は本質的に人間支援ツールであり、法的な人格属性は認められないと主張する。人工知能は、機械を人間のように考えて独立自主学習の能力を獲得することを目標としているが、その行為は、あらかじめ設定されたプログラムに従って実行する場合でも、プログラミングから離れた自主的な実行の場合であっても、法規範が能力に従う意思性に欠け、客観的に法益侵害の結果をもたらしても、刑法上の責任性が認められないとする[16]。

では、AI 詐欺の文脈では、どのような対応や議論を展開する必要があるのだろうか。現在では、AI 詐欺犯罪の中で、最もよく見られる人工知能は、第三者決済や新型支払い、例えば WeChat ペイ、アリペイなどの機械やロボットである。これらの支払い方式で、振込アリペイの引き出しなどの経済活動を行う過程で、従来の支払い方式における人の目で脳を認識して判断する必要はなく、正しいアカウントとパスワードを入力するだけで直接機械の知能識別と検証を通じて取引を完成することができる。また、このような識別と認証機能は人間の脳の識別と判断過程と同じであり、しかも人間の脳よりもっと正確で迅速である。

以上の問題意識に基づき、ランダムに中国裁判文書網上から 100 例のサイバー詐欺事件をサンプリング調査したところ、そこから得られた結果をグラフにすると、以下のようになる。

15) 刘宪权《人工智能时代的刑事风险与刑法对应》、《法商研究》2018 年第 1 期。
16) 时方《人工智能刑事主体地位之否定》《法律科学（西北政法大学学报）》2018 年第 6 期 第 71 页

第三者支払い	68
混合	11
他の方法	9
ATM	7
銀行の窓口	5

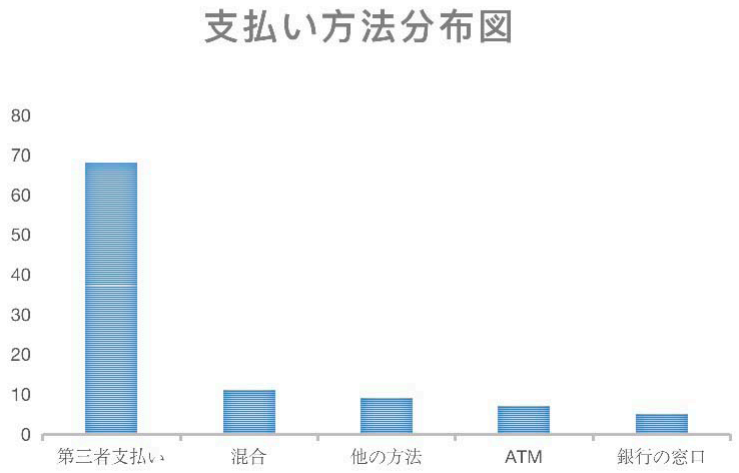

図 2

大量の既発事件から、財産性ネット口座（例えばアリペイ、WeChat ウォレットなど）は常にサイバー詐欺行為をめぐる中心であり、狙われる目標であることが判明する。それゆえ、財産性ネット口座の法的性質が、まず明確にすることが問題となる。現状では、法律規定や認識が統一されていないため、実務ではこのような事件に対する判断も統一されていない。

例えば、以下に示す、2015 年の 2 つの例がそのことを示している。

一つ目の事件は、徐某が職場から配布された業務用携帯電話を使用した際に、その携帯電話上のアリペイアプリが被害者の馬某の口座に直接登録できることに気づき、その口座内には 50,000 元余りの残高があった。徐某は、この金銭に誘惑され、その携帯電話を利用して馬某口座残高内の 15,000 元を劉某の銀行口座に振り替え、劉氏が銀行カードからお金を引き出して、徐某に渡した。

寧波市海曙区検察院は徐某被告を窃盗罪の疑いで人民法院に起訴し、海曙区裁判所は徐某被告詐欺罪が成立したと認定し、懲役7カ月、猶予刑1年を言い渡し、罰金3,000元の判決を下した。一審判決後、海曙区検察院は、有罪判決の誤りを理由に寧波市中級人民法院に控訴したが、中級人民裁判所は、原判決を維持すると判断した[17]。

もう一つの事件は、廖氏は、被害者の某氏が食事をしている間に、某氏がホテルに残していたカバンを家に持って帰った。ランドセルの中で廖氏は被害者の携帯電話を発見し、廖氏は被害者がインストールしていたアリペイソフトをクリックし、その口座に紐付けられた銀行カードから7,000元を本人口座に送金した、というものである。佛山市順徳区検察院は、窃盗罪で廖氏を起訴し、順徳区裁判所は窃盗罪と認定し、廖氏に拘役6カ月を言い渡し、罰金1,000元の判決を下した。事件の判決後、、某は自分の行為は窃盗罪に該当しないと考え、原判決を不服として控訴したが、仏山市中級人民裁判所は、原判決を維持すると判断した[18]。

この中で、アリペイのような第三者決済プラットフォームの定性が問題となっている。一般的に、詐欺罪における“交付”は主観客観行為の統一体であり、偽りを受けて客観的に財物の占有を移転することを要求し、また、人を騙すことによって主観的に特定の財物に対して引渡し占有の認識を持つことを要求する。詐欺罪と認定されれば、つまり詐欺犯が騙したのはアリペイプラットフォームであり、プラットフォームは財物の受け渡し状況を知っている一方で、被害者は、自分の財物の交付移転を知らないのである。それゆえ、錯誤に陥ったのもアリペイであって、被害者ではないで、これは伝統的な三角詐欺に似ている。

この場合、アリペイの刑事主体性を肯定してもよいのであろうか。中国刑法理論では、窃盗罪と詐欺罪の本質的な違いの一つは、窃盗罪が“能動獲得型”

17) 浙江省寧波市中級人民法院（2015）の刑二終字第497号刑事判決書を参照。
18) 広東省仏山市中級人民法院（2015）仏中法刑二終字第100号刑事判決書を参照。

犯罪であり、詐欺罪が“受動交付型”犯罪であることであると考えられている。換言すれば、詐欺と秘かな財物取得が並行する財産侵害事件をどのように認定するかについては、詐欺罪の“受動交付”と窃盗罪の“能動的獲得”を正確に解釈することが、窃盗罪と詐欺罪を区別する鍵となる[19]。すなわち、窃盗は、他人が知らないうちに密かに盗取するものである。窃盗罪と認定されれば、行為者が他人の第三者決済口座を詐称して支払い、振込などの行為を行う場合、行為者が第三者プラットフォームに対して資金調達指令を開始したことに相当し[20]、行為者は、必ずその財産侵害行為の全過程が第三者支払いプラットフォームに対して公開されていることを知っている。そのように考えると、密かな窃取でもないようである。

II. 帮助犯の認定の困難性

AI 技術の発展は、犯罪コストを下げると同時に犯罪効率を向上させ、サイバー犯罪の派生は、分業の様相を呈している。細分化傾向により、各犯行が独立、各段階の責任者が明確な犯罪利益チェーンが形成された。サイバー詐欺犯罪チェーンにおけるネットワーク幇助行為の地位は比較的独立しており、正犯行為の発生を加速させるとともに、幇助犯が最も利益を得ている。サイバー犯罪の重要な特徴は、グループ犯罪であるということである。事件の多くは、サイバー上での共同犯罪である。幇助犯は、他人のサイバー詐欺行為を知りながら、他人を幇助している。主観的には、サイバー詐欺の幇助の故意がある者である。詐欺行為者と幇助犯とでは、共同犯罪の故意があれば、この幇助行為は詐欺罪のそれと認定されることになる。両者は、サイバー詐欺の共犯であると認定されることになる。

しかし、幇助犯の認定は難しい。まず、AI 技術支援者と犯罪実行行為者の

19）徐光华《刑法解释视域下的“自愿处分”——以常见疑难盗窃与诈骗案件的区分为视角》，载《政治与法律》2010 年第 8 号

20）刘宪权《论新型支付方式下网络侵财犯罪的定性》《法学评论（隔月刊）》2017 年第 5 号（总 205 号）。

多くは、異なる犯罪段階に分かれており、ネットワークの仮想性により、両者のつながりも疎である。そして、犯罪者は細分化された分業により、犯罪因果チェーンを長くした。現在では、チームが分担利用してネットワーク運営を行うことが多い。その中には、犯罪者が多く、犯罪に関連する部分が多く、犯罪地域が広く、関連部門が多く、犯罪事実に関連するものが多い。捜査中に捜査員がこれらの関係者すべてを逮捕することは困難であり、タイミングが把握しにくく、全力を尽くしても、往々にして全力を尽くすだけに終わってしまう可能性がある。ネット犯罪のうちの一部の犯罪被疑者だけを逮捕したにとどまり、多くの幇助者は全く逮捕されないこともよくある。そのため、犯罪の不法利益への誘惑に加えて、ネット犯罪業の自己修復能力が強く、すぐに息を吹き返し、捜査遂行中のネット関連の犯罪は防ぎきれず、打撃を受けていない受動的な行動を招く可能性がある。

また、既存の法律の AI 詐欺の幇助犯への適用にも問題がある。中国の《コンピュータ情報システム解釈》第 9 条[21]の規定に対して、ある学者は、上記の司法解釈が、特定のサイバー犯罪支援行為に対して共犯者を成立させるモデルについて、“他人が特定の犯罪を実施していることを知っていること + 依然として特定のネットワーク情報技術支援行為を提供すること + 特定の深刻なエピソードを備えている = 共同犯罪に属する（認定、成立）共同犯罪”にまとめた[22]。さらに、中国刑法第 287 条の 2 の「情報ネットワークに犯罪活動の幇助の罪」の規定によると、他人が情報ネットワークを利用して犯罪を実行していることを明確に知りながら、その犯罪のためにインターネット接続、サーバーの受託管理、ネットワーク・メモリーまたは通信転送等の技術的支援を提供し、または広告を展開し、支払決済等の援助を提供した者は、最高で 3 年の懲役であるとされている。

しかしながら、幇助行為はサイバー犯罪の中心的な一環であり、また、幇助

21） 具体的な条文の内容は後掲【条文資料】に掲記する。

22） 于志刚：《网络空间中犯罪帮助行为的制裁体系与完善思路》、《中国法学》2016 年第 2 期。

行為の背後に隠された社会的有害性は巨大である。それゆえ、このような処罰は、“罪刑均衡原則”に合わないと考える。

III. 個人情報の問題

サイバー犯罪は、情報と深く関連した犯罪でもある。サイバー詐欺は、一般に他人の個人情報を操作して、他人を騙す行為であることが多いように思われる。すなわち、行為者は、虚偽の情報を作出して、または真実の情報を隠匿して、被害者を騙しているのである。最初にも述べたように、AI は個人情報やデータの収集処理に大きな利便をもたらし、詐欺の遂行過程を容易にし、結果をさらに深刻化させている。したがって、個人情報の保護は、非常に重要だと認められる。

現在のところ、中国ではまだ“個人情報保護法”が制定されていない。個人情報の保護に関する規定は、刑法、民法、インターネット安全法など法律、行政法規あるいは解釈性規定の中に点在しているという状況にある。ただし、個人情報の保護を明確化する前に、まず、法律上、個人情報の範囲を明確化しなければならない。

2013 年 4 月 23 日、最高人民裁判所と最高人民検察院と公安部は《公民の個人情報の侵害について法律で処罰する活動的な通知》を発布した。この通知において、個人情報として、公民の名前、年齢、有効な証明書番号、婚姻状況、職場、学歴、履歴、家庭住所、電話番号など、公民の個人身分を識別するもの、または公民の個人のプライバシーに関するものを含めている。この規定によるならば、個人情報とは、公民の個人身分を識別されたもの、または公民の個人のプライバシーに関するもの、であることになる。

しかし、サイバー詐欺の事案では、行為者は、被害者の銀行カード（キャッシュカード）の情報やアリペイなどの電子決済の情報などを利用することがよくある。これらの情報は、個人の身分に関する情報である、あるいは個人のプライバシーであると認定することは困難である。そのため、2016 年 11 月 7 日に、《インターネット安全法》第 76 条第 5 項が規定され、個人情報とは、電子的にまたは他の方法で単独であるいは他の情報と照合して、自然人の個人の

身分を識別される情報であるとされた。たとえば、公民の氏名、年齢、有効な証明書番号、家庭住所、電話番号を含むが、これらに限られるわけではない。しかし、この規定は、個人身分の識別を重視するものであるため、個人情報とされるものの範囲が狭くなっている。

そこで、2017 年 6 月 1 日、最高人民裁判所と最高人民検察院は《公民の個人情報の侵害の刑事案件に関する法律適用の若干問題の解釈》を発布した。この規定によれば、個人情報とは、電子的または他の方法で単独あるいは他の情報と照合することにより、自然人の個人の身分を識別された、あるいは、特定の自然人の活動状況を反映した情報であるとされる。この定義は、たとえば、公民の名前、年齢、有効な証明書番号、家庭住所、電話番号、財産状況、行動軌跡などを含めている。

この解釈は、一応、個人情報の範囲を規定したものではある。しかしながら、刑法上の“個人情報”の認定は、まだ不明瞭なところが多いように思われる。

2. 検討

刑法による、AI を利用した詐欺行為の規制については、他国ではすでに異なる立法実践がある。その中で典型的なのは、ドイツ刑法 263 条のように、「自分や第三者が不法利益を得るために、他人のコンピュータプログラムを不正確に調整し、不正確または不完全なデータを使用することで、データを不正に使用することである。あるいは他の手段が他人のコンピュータプログラムに不正な影響を与え、他人の財産をそのために損失を受けた場合は、5 年以下の自由刑または罰金を科す」と規定する例である[23)]。一方、日本の刑法第 246 条の 2 も、他人が事務を処理する計算機に不実の情報を入力し、不実の電磁記録を作成し、財産上の不法利益を取得することを電子計算機使用詐欺罪としている。その他、中国台湾地区も、1988 年に“刑法”第 339 条の 2 を新設し、自己または第三者の不法の所有を意味することを規定し、不正な方法で自動支払

23)《ドイツ刑法典》[M]. 徐久生，庄敬華，訳．北京：中国法制出版社、2000。

設備から他人の物を取得する構成で電脳詐欺罪、財産上不法利益罪を規定している[24]。こういった規定を採用したのは、ドイツや日本が、機械は騙されないという原則に基づいているからである。機器が騙されることを認めることで詐欺罪の定型性が失われてしまい、窃盗罪との区別が困難になると考えられているのである。また、一般的には、このような行為は詐欺罪に近いため、コンピュータ詐欺罪という罪を設けてこのような犯罪を加える必要がある。

中国には、まだ特別な規定が存在しないが、2008 年 4 月 18 日最高人民検察院“他人のクレジットカードを拾って ATM 機で使用する行為がどのように定性的かに関する問題の返答”、他人のクレジットカードを拾って ATM 機で使用する行為は、刑法第 196 条第 3 項に規定する“他人のクレジットカードを詐称する”場合に属し、犯罪を構成し、クレジットカード詐欺罪で刑事責任を追及することになる。2009 年 12 月 3 日最高人民法院、最高人民検察院“クレジットカード管理妨害刑事事件の処理に関する具体的な法律のいくつかの問題の解釈を適用する”第 5 条も同様の規定を行っている。

この規定は、ATM が騙されることを肯定している。機器が騙されるかどうかはともかく、ATM をある程度において「道具人」にしようとするものである。ATM 機の代わりに銀行員の人間が引き出し、貯金、振替送金などの金融業務を処理していると仮定し、また ATM 機がないと仮定すると、銀行営業所の従業員は依然として引き出し、貯金、振込送金などの金融業務を処理しており、ATM 機の引き出しだけで金融業務の処理をより便利にし、よりスマートにしている。これは安全装置の知的ロックのような機械的なことではない。

そうであれば、同じ弱い人工知能の新しい決済プラットフォームなどの問題も、そのように認定できるのではないかとも思われる。ただし、ATM よりアリペイなどの新しい決済プラットフォームはより複雑であるため、中国の法律では、これに対応する必要があると考える。例えば、新しい罪や詳細な司法解

24）　赵秉志、周加海：《台湾地区现行刑法改正典修正内容简介》、《云南大学学报（法学版）》2003 年第 4 期。

釈を増やして規制するといったことである。人工知能が発展して、強い人工知能の段階に至れば、人工知能に法的主体の地位を与える必要があるかもしれない。しかしながら、少なくとも、現行の刑事司法の問題に関する限り、処罰される対象者も、処罰を決定する者も「人」であると考えるべきである[25)]。法律は事態に応じた改善・前進をしていく必要はあるが、AIに法人格を与えることを考えるのは、まだ時期尚早であると思われる。

また、個人情報保護も十分に重視する必要があり、AI詐欺を根源から管理するためには、個人情報保護が重要である。さらに、実務において、AI詐欺捜査活動では、次のような問題に多く遭遇しやすい。例えば、一部の被害者は責任を追及しようとは思わず、証拠を与えようとしない。あるいは、警察はAIの知識がわからない者も一定数いるので、捜査が難しい。また、いくら事件を解決しても、騙された金を取り戻すのは難しい。さらに、青少年の方が人工知能に触れやすいため、上記のランダム調査事件でも、AI詐欺に参加している青少年も少なくないことがわかる。しかし、年齢制限で責任を追及できないなど、この一連の問題にも中国の法律の検討の必要性が重視されており、相応の対策が必要である。

四、終わりに

AIの発展は、現在も、また今後も比較的長期間にわたり、弱い人工知能時代にあるが、AIの能力や、そのもたらす威力は巨大である。AIは、詐欺のような財産犯罪に重大な影響を与えるだけでなく、生活のあらゆる面にも作用することができる。AIのリスク防止問題を重視しなければならないことは、疑いようもない。もし行為者が人工知能を濫用すれば、このような行為の社会的危害性は、完全にコントロールが困難となり、財産権が侵害されるだけではなく、国家、公共安全が脅かされるほどの可能性がある。

25) 星・前掲注（10）論文。

そのため、刑法は人工知能を濫用する行為を規制しなければならず、刑法以外の法律法規の規制では、人工知能製品の研究開発者や利用者を抑止するには不十分であり、人工知能リスクの防止作用を十分に果たすことができない。刑法は、犯罪者の権利の剥奪は往々にして不可逆的であり、明らかな警告作用を果たすことができる。しかし同時に、刑法は最後の解決手段であり、刑法の抑止力が期待される場合であっても、刑法の謙抑性も同時に考慮する必要がある。立法者も、犯罪の範囲を慎重に拡大すべきであり、ある種の社会に危害を及ぼす行為に対しては、他の法律が規制や調整に不十分な場合にのみ、刑法はそれを調整の範囲に入れつつ、犯罪と規定することができる。

このような観点に基づきつつ、今後もさらに研究を進めていくことを約して、一旦擱筆する。

【条文資料】添付の中国のサイバー詐欺に関する法規定

1. ＜刑法＞の基本規定

第 266 条「詐欺罪」

公私の財物を騙取して、その金額が多額である場合、3 年以下の懲役、拘役若しくは管制に処し、罰金を併科し、又は罰金のみに処する；金額が巨額である、又は他の重大な情状がある場合、3 年以上 10 年以下の懲役に処し、罰金を併科する；金額が特別に巨額である、又は他の特別に重大な情状がある場合、10 年以上の懲役若しくは無期懲役、罰金又は財産の没収を併科する。本法は、他の規定があれば、他の規定による。

2. ＜刑法＞のその他の規定

1＞、第 265 条「窃盗罪」

不法にコンピューター情報システムへ侵入又はコントロールするため、専門的プログラム、工具などを提供し、若しくは、他人の不法にコンピューター情報システムをコントロールした違法的な行為であることを知りながら、プログラム、工具などを提供したら、重大な情状がある場合、前項の規定により処罰する。

組織が前項の罪を犯した場合には、組織を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

2＞、第 285 条「コンピューター情報システム侵入罪、コンピューター情報システムのデータ不法所得不法管理、コンピューター情報システムのデータ不法取得不法管理ソフト道具供与罪」

1、国家の規定に違反し、国の事務、国防建設又は先端科学技術領域のコンピューター情報システムに侵入した者は、3 年以下の懲役又は拘役に処する。

2、国家の規定に違反し、前項以外のコンピューター情報システムへ侵入し、又はその他の技術手段を通じて、このコンピューター情報システム中で保存、処理若しくは転送的なデータを取得し、又は、このコンピューター情報システムに対し不法なコントロールした者は、重大な情状がある場合、3 年以下の懲役若しくは拘役に処し、罰金を併科し、又は罰金のみに処する。特別に重大な情状がある場合、3 年以上 7 年以下の懲役に処し、罰金を併科する。

3、コンピューター情報システムへの侵入又は不法なコントロールするために専ら用いられるプログラム若しくは手段を提供し、又は、他人の不法にコンピューター情報システムをコントロールする違法行為を明確に知りながら、その者のためにプログラム又は手段を提供した者は、重大な情状がある場合、前項の規定により処罰する。

4、組織が前項の罪を犯した場合には、組織を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

3 >、第 286 条「破壊コンピューター情報システム罪」

1、国家の規定に違反し、コンピューター情報システム機能に対して、削除し、変更し、増加し又は干渉して、コンピューター情報システムの正常な実行を不能にして、重大な結果をもたらした者は、5 年以下の懲役または拘役に処する。特別に重大な場合には、5 年以上の懲役に処する。

2、国家の規定に違反し、コンピューター情報システムにおける保存、処理、又は転送のデータと応用プログラムに対して、削除、変更、増加の操作をした者は、重大な情状である場合、前項の規定により処罰する。

3、コンピューター・ウィルス等の破壊的プログラムを故意に作成し、伝播し、コンピューター情報システムの正常な実行に影響及ぼした者は、重大な情状である場合、第一項の規定により処罰する。

4、組織が前 3 項の罪を犯した場合には、組織を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

4 >、第 286 条の 1「情報ネットワーク安全管理義務の履行を拒否する罪」

ネットワーク・サービス提供者が、法律や行政法規の規定による情報ネットワーク安全管理義務を履行せず、監督管理部門による是正措施を命令して、また拒否して是正しないまま、下記の情状の一があれば、3 年以下の懲役、拘役若しくは管制に処し、罰金を併科し、又は罰金のみで処する。

(1)　違法情報を大量に伝播させること。

(2)　ユーザーの情報を漏洩させて、重大な結果をもたらしたこと。

(3)　刑事事件の証拠を滅失させて、重大な情状があったこと。

(4)　その他重大な情状があったこと。

2、組織が前項の罪を犯した場合には、組織を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

3、前 2 項の行為を行い、同時にその他の犯罪も構成する場合、その処罰は、より重い規定により罪を定め、処罰する。

5 >、第 287 条の 1「情報ネットワークを違法に利用する罪」

情報ネットワークを違法に利用して、下記の情状の一があれば、3 年以下の懲役若

しくは拘役に処し、併科し、又は罰金のみに処する。

(1) 詐欺の実行、犯罪方法の伝授、違法禁止物品若しくは管制物品の作成又は販売等のためにウェブサイト又は通信グループを設立する行為。

(2) 麻薬、銃器、及び猥褻物等の違法禁止物品、管制物品の作成若しくは販売、又はその他違法犯罪に関する情報を発信する行為。

(3) 詐欺等の違法犯罪の活動を実行するために、情報を発信する行為。

2、組織が前項の罪を犯した場合には、単位を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

3、前2項の行為を行い、同時にその他の犯罪も構成する場合、その処罰は、より重い規定により罪を定め、処罰する。

6＞、第287条の2「情報ネットワークに犯罪活動の幇助の罪」

他人が情報ネットワークを利用して犯罪を実行していることを明確に知りながら、その犯罪のためにインターネット接続、サーバーの受託管理、ネットワーク・メモリーまたは通信転送等の技術的支援を提供し、又は広告を展開し、支払決済等の援助を提供した者は、3年以下の懲役、若しくは拘役に処し、罰金を併科し、又は罰金のみに処する。

2、組織が前項の罪を犯した場合には、組織を罰金に処し、かつ、その直接に責任を負う主管者その他直接責任者を前項の規定により処罰する。

3、前2項の行為を行い、同時にその他の犯罪も構成する場合、処罰は、より重い規定により罪を定め、処罰する。

刑事司法の調整の規定

《詐欺刑事事案に関する具体的問題の適用の解釈》

第1条　騙取された公私の財物の価値は3千元か1万元以上、3万元か10万元以上、50万元以上、これはそれぞれが、刑法第266条に規定する“金額が多額”、“金額が巨額”、“金額が特別に巨額”と認定しなければならない。(中国の1千元～日本の1万8千円)

地方によって、高級裁判所、検察庁は当該地区の経済や発展状況などにより、前項に規定した金額幅のなかで、共同で研究して、当該地区で実行している具体的金額を定めて、最高裁判所、最高検察庁に報告して記録にとどめる。

第2条　騙取された公私の財物の価値は、前条の解釈の標準に達していて、下記の情状の一があれば、刑法の第266条の規定により、裁量により重い処罰を科すことができ

る。

(1)、メール、電話又はインターネットを利用し、放送局、新聞などを通じて、虚報を発信し、不特定多数者に対して詐欺をすること。

(2)、災害の緊急救助、特別なケア、貧困家庭や貧困地区に対し援助、移民、救済、医療の財物に対して詐欺をすること。

(3)、被災者を救済するためのカンパの名をもって詐欺をすること。

(4)、身体障害者、老人若しくは労働能力を喪失した人を対象として詐欺をすること。

(5)、被害者の自殺、心神喪失をもたらした、またはその他重大な結果をもたらしたこと。

騙取された金額は本解釈第 1 条に規定した“金額が多額”、“金額が巨額”、“金額が特別に巨額”の標準に接近し、かつ、前項が規定の情状の一がある、若しくは詐欺グループの緊要な人、これは、それぞれ刑法第 266 条に規定した“他の重大な情状”、“他の特別に重大な情状”と認定しなければならない。

第 5 条　詐欺未遂、金額巨大の財物を目標して、または他の重大な情状があれば、処断して罰すべきである。

電話やメールやインターネットなど電信技術手段を利用して、不特定多数人に詐欺を実施して、金額の検証しにくい場合、以下の情状の 1 があれば、刑法の第 266 条のほかの重大な情状”と認定しなければならない、詐欺罪（未遂）と断罪する。

(一)、5000 条以上の詐欺メッセージを送ること；

(二)、500 人次の詐欺電話をすること；

(三)、詐欺手段が悪い、危害が厳重的なこと。

《サイバー詐欺に関する刑事事件の若干的問題の法律の適用の意見》

第 1 条　騙取された公私の財物の価値は 3 千元以上、3 万元以上、50 万元以上、これはそれぞれが、刑法第 266 条に規定した“金額が多額”、“金額が巨額”、”金額が特別に巨額”と認定しなければならない。

この規定は上述の解釈の規定した金額の最低数を取った。

(二)、第 2 条、サイバー詐欺を実施して、騙取された公私の財物の価値は、前条の解釈の標準に達していて、下記の情状の一があれば、裁量により重い処罰を科すことができる。

①、被害者または近い親族の自殺屋や死亡、あるいは心神喪失など重大な結果をもたらしたこと；

②、司法機関など国家機関の従業員と偽称して、詐欺を実施すること；

③、サイバー詐欺シンジケートの組織、指揮；

④、域外でサイバー詐欺を実施すること；

⑤、サイバー犯詐欺の為刑事処罰を受けた、また 2 年内でサイバー犯詐欺の為行政処罰を受けたこと；

⑥、身体障害者、老人、未成年人、在校学生、労働能力が喪失した人を対象として詐欺をすること、若しくは、重病患者また他の親族の財物を詐欺すること；

⑦、災害の緊急救助、特別なケア、貧困家庭や貧困地区に対し援助、移民、救済、医療の財物に対して詐欺をすること；

⑧、被災者を救済するや募金などためのカンパの名をもって詐欺をすること；

⑨、電話追呼システムなど技術手段を利用して、厳重に公安機関など部門の仕事を干渉すること；

⑩、フィッシングや木馬プログラム、ウェブ浸透リンクなど隠蔽な技術手段を利用して詐欺をすること。

ここは十種の加重情状を増設した。

（三）、サイバー詐欺をして、犯罪容疑者、被告人は財物を騙取った、詐欺罪（既遂）を処罰する。金額の検証しにくい場合、以下の情状の 1 があれば、刑法の第 266 条のほかの重大な情状”と認定しなければならない、詐欺罪（未遂）と断罪する。

①、5000 通以上の詐欺メッセージを送ること、または 500 人次の詐欺電話をすること；

②、インターネットで詐欺情報発布して、ネットサーフィン量は 5000 次以上。

前項に規定した行為を実施して、数は前項の（一）、（二）の規定した量の 10 倍以上、刑法の第 266 条のほかの特別な重大な情状”と認定しなければならない、詐欺罪（未遂）と断罪する。

ここは解釈より、ネットサーフィンを増加して、ほかの重大な情状を補充した。

(4)、他人のサイバー詐欺することを知りながら、以下の 1 つ情状があれば、共同犯罪に処する、でも、法律や司法解釈の他の規定があるは除外する。

①、クレジットカード、資金支払い決済口座、テレホンカード、通信手段の提供；

②、公民の個人情報を不法に取得する、販売する、提供すること；

③、フィッシングや木馬プログラムなど悪いプログラムの制作、セールス、提供；

④、偽基地局と相関サービルの提供；

⑤、インターネット接続、サーバーの受託管理、メモリー容量、通信転送アクセスなど技術的支持を提供し、または支払決済等幇助の提供；

⑥、番号の変更ソフトや通話線路など技術サービルを提供する場合、番号（caller ID）

を修正されて、国内党政機関や司法機関や公共サービス部門の番号になって、または域外番号は域内番号になったことを知りながら、サービスを提供すること；

⑦、資金、場所、交通、生活保障など幇助を提供すること；

⑧、詐欺犯罪の所得とこの所得によりもらった利益の移転を幇助して、套現（convert into cash）、取現（enchashment）。

《コンピュータ情報システム解釈》

第九条　他人が刑法第 285 条、第 286 条に規定する行為を実施していることを知りながら、次のいずれかを有する場合は、共同犯罪と認定し、刑法第 285 条、第 286 条の規定により処罰しなければならない。

（一）コンピュータ情報システムの機能、データ又はアプリケーションを破壊するためのプログラム、ツールを提供し、違法に得られた 5 千元以上、又は 10 人以上を提供する。

（二）インターネットアクセス、サーバホスト、ネットワーク記憶空間、通信伝送路、費用決済、取引サービス、広告サービス、技術訓練、技術支援などの支援を提供し、違法に 5 千元以上を所得する。

（三）ソフトウェアの普及を依頼し、広告を投入するなどして 5 千元以上の資金を提供する。

前項の規定による行為を実施し、数量又は額が前項の規定基準の 5 倍以上に達した場合は、刑法第 285 条、第 286 条に規定する“筋が特に深刻”又は“結果が特に深刻”と認定しなければならない。