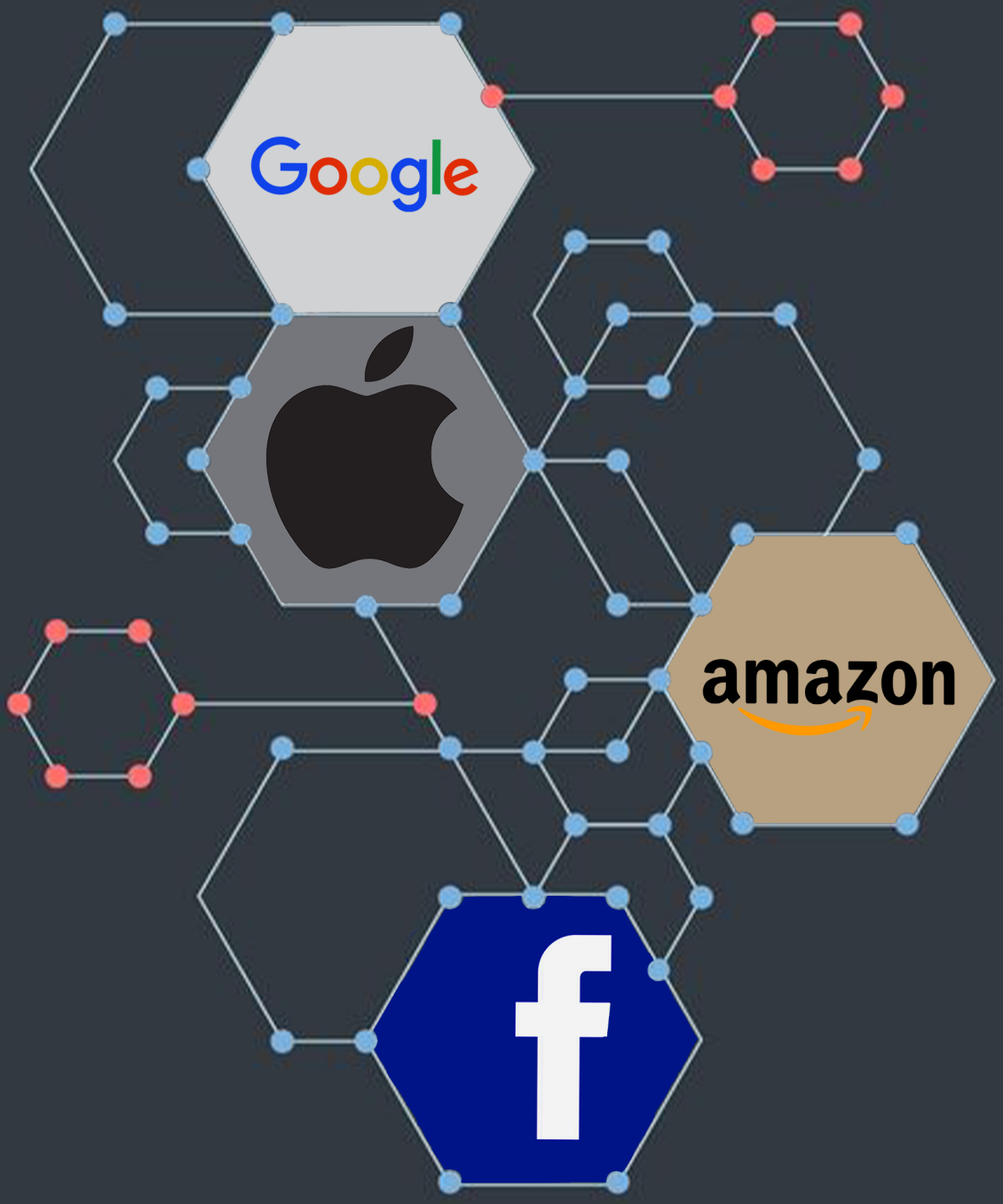

RCEP इलेक्ट्रॉनिक कॉमर्स अध्याय और TPPA में जरूरी अंतर एवं ई–कॉमर्स के लिये WTO में दिये जरूरी सबक

प्रोफेसर जेन केल्सी, विधि संकाय,
ऑकलैंड विश्वविद्यालय,
न्यूजीलैंड

RCEP *इलेक्ट्रॉनिक कॉमर्स अध्याय और* TPPA *में जरूरी अंतर एवं ई–कॉमर्स के लिये* WTO *में दिये जरूरी सबक#*

रीजनल कॉम्प्रिहेंसिव इकनोमिक पार्टनरशिप(RCEP) का इलेक्ट्रॉनिक कॉमर्स अध्याय अब मुहैया करा दिया गया है। इसमें जो लिखा गया है वह जरूरी है, क्योंकि RCEP ट्रांस–पैसिफिक पार्टनरशिप एग्रीमेंट के बाद से पूरे होने वाले दो बहु–क्षेत्रीय समझौतों में से एक है। TPPA को डिजिटल व्यापार के नए वैश्विक नियमों के टेम्पलेट के रूप में बढ़ावा दिया गया है। इसके बाद हुए यूएस कनाडा मैक्सिको एग्रीमेंट(USMCA) ने TPPA के डिजिटल व्यापार नियमों में बढ़ोतरी कर दी और पहले से ही ताकतवर टेक्नोलॉजी कॉर्पोरेशन को और ज्यादा व्यापक आश्वासन और फायदे पहुँचाने का काम किया। RCEP ने उन वृद्धियों पर रोक लगाने का काम किया है।

RCEP के 16 वार्ता दलों में से 6 TPPA के हस्ताक्षरकर्ता भी हैं। इसके अलावा इसमें वर्ल्ड ट्रेड ऑर्गनाइजेशन(WTO) में इलेक्ट्रॉनिक कॉमर्स के जॉइंट स्टेटमेंट इनिशिएटिव(JSI) के 3 कोऑर्डिनेटर: ऑस्ट्रेलिया, सिंगापोर और जापान भी शामिल हैं। RCEP के अन्य दलों में चीन, और हाल ही में शामिल हुआ भारत भी है, जिनके डिजिटल डोमेन के नियमों के संदर्भ में पक्ष और विपक्ष के हित हैं। इसमें इंडोनेशिया और वियतनाम जैसे आसियान देश भी शामिल हैं, जो लंबे प्रत्यक्ष रूप से डाटा और डिजिटल लेनदेन को नियंत्रित करते रहे हैं।

लंबी बातचीत के बाद, माने गए RCEP टेक्स्ट में TPPA ई–कॉमर्स अध्याय के कई मुख्य तत्वों को या तो छोड़ दिया है या उसमें काफी बदलाव कर दिए हैं और अब वह लागू करने लायक नहीं है। TPPA टेम्प्लेट से पीछे हटने की यह प्रक्रिया अपने नियमों के निहितार्थ की अधिक परिपक्व समझ और सरकारों को डिजिटल डोमेन को विनियमित करने के लिए प्रभावी नीति स्थान बनाए रखने की आवश्यकता को दर्शाती है। हालांकि इस अध्याय से अभी भी चिंताएं पैदा होती हैं, और यह उन बुनियादी सवालों का जवाब देने में भी नाकाम है, जिसके तहत यह आपत्ति जताई जाती है कि इंटरनेट गवर्नेंस, डाटा, प्रतिस्पर्धा और निजता के साथ किसी भी भी कीमत पर 'व्यापार' की आड़ में समझौता नहीं होना चाहिये।

हालांकि एक प्रसिद्ध बयान है कि RCEP में दलों का स्थान, उनके WTO में स्थान की वजह से पूर्वाग्रह से ग्रस्त नहीं होता है। लेकिन RCEP के मसौदे में एक अहम बात पर रौशनी डाली गई है कि WTO में देशों पर ई–कॉमर्स को लेकर समझौता करना का बेहद दबाव रहता है।

क्यों RCEP से बेहतर है TPPA

RCEP *और* TPPA *के बीच 5 बुनियादी फर्क यह हैं*

1 RCEP *ई–कॉमर्स अध्याय राज्य–राज्य विवाद निपटान द्वारा लागू करने योग्य*

1# प्रोफेसर जेन केल्सी, विधि संकाय, ऑकलैंड विश्वविद्यालय, न्यूजीलैंड, ११ फरवरी २०२०। यह विश्लेषण रीजनल कॉम्प्रिहेंसिव इकनोमिक पार्टनरशिप(RCEP) के इलेक्ट्रॉनिक कॉमर्स अध्याय के अंतिम संयुक्त टेक्स्ट को संदर्भित करता है, जो कि यहाँ देखा जा सकता है https://bilaterals-org/?rcep&e&commerce&chapter-text-41085

नहीं है। (अनु. 17) भविष्य में 5 साल(जिसे आम समीक्षा का समय माना गया है) के दौरान लागू करने की अनुमति देने के लिए हुए किसी भी समझौते के दायरे में सिर्फ वही दल आएंगे, जिन्होंने सहमति जताई है। व्याख्या और अनुपालन के बारे में पार्टियों के बीच विवाद केवल पार्टियों की जॉइंट कमेटी का संदर्भ और अच्छे विश्वास परामर्श के अधीन हैं।

2 *इसमें सोर्स कोड को लेकर कोई प्रावधान नहीं हैं।* जबकि TPPA पार्टियों को मालिकों से सोर्स मांगने और उसके लीक होने से रोकने का काम करता है। सिर्फ उस काम के अलावा जहाँ जटिल इंफ्रास्ट्रक्चर बन रहा है। हालांकि इंटेलेक्चुअल प्रॉपर्टी अध्याय में अभी भी कुछ बड़े व्यापार रहस्यों के प्रावधान हो सकते हैं।

3 *डेटा ऑफशोर के ट्रांसफर के लिए कवर किये गए व्यवसायों के अधिकार, और एक पार्टी क्षेत्र के अंदर सर्वर खोजने या इस्तेमाल करने की उनकी जरूरत पर प्रतिबंध लगाने को एक आत्म–आंकलन करने वाले सार्वजनिक नीति परीक्षण के अधीन कर दिया जाता है।(अनु. 15–16)* हालांकि, इस उपाय को अपनाने की जरूरत को ही आत्म–आंकलन की जरूरत है, सार्वजनिक नीति उद्देश्य के लिए इसकी जरूरत नहीं है। उपाय में मनमाने या अनुचित भेदभाव का साधन भी नहीं होना चाहिए(इसमें सिर्फ विभिन्न राष्ट्रीयता ही नहीं, तकनीक या विभिन्न प्रकार के डेटा भी शामिल हो सकते हैं) या इसमें व्यापार पर प्रतिबंध का गठन भी नहीं होना चाहिये (जो तब नुकसानदेह हो सकता है जब उपाय से निजी हित हो रहा हो)।

4 *डेटा और लोकल कंप्यूटिंग सुविधाओं के ट्रांसफर का दायित्व भी पूरी तरह से आत्म–आंकलन और अविवादित राष्ट्रीय सुरक्षा अपवाद के अधीन है।* एक पार्टी ऐसा कोई भी उपाय अपना सकती है, जिसे वह अपने सुरक्षा हित के लिये जरूरी मानती है, और बाकी पार्टियाँ ऐसे किसी उपाय पर विरोध नहीं जता सकती हैं। अभी पूरे RCEP के आम सुरक्षा अपवाद के बारे में किसी को जानकारी नहीं है। हालांकि, इन उपायों में दिए गए किसी भी विवाद में स्पष्ट सुरक्षा के बारे में यही कहा गया है कि ऐसा भी हो सकता है कि आम सुरक्षा प्रावधान में, कोई समतुल्य सुरक्षा हो ही नहीं सकती है।

5 *इलेक्ट्रॉनिक ट्रांसमिशन पर लगने वाले सीमा शुल्क पर लगी रोक को स्थायी नहीं किया गया है। (अनु. 12)* यह अभ्यास इलेक्ट्रॉनिक कॉमर्स पर WTO वर्क प्रोग्राम से संबंधित WTO मंत्री सम्मेलन के निर्णयों के अनुसार स्पष्ट रूप से तैयार किया गया है। इस RCEP का प्रावधान के समायोजन को आगे होने वाले वर्क प्रोग्राम पर मंत्रियों के निर्णयों से संबंधित रखा गया है – न कि बहुपक्षीय JSI वार्ताओं से जोड़ कर। अगर WTO की स्थगन प्रक्रिया में कमी आती है, जैसा कि कुछ विकासशील देशों ने दिसंबर 2019 में इसके नवीकरण पर चर्चा के दौरान प्रस्तावित किया था, तो कोई भी RCEP पार्टी अपने अभ्यास को स्थिति के अनुकूल एकतरफा रूप से समायोजित कर सकती है।

RCEP *में अन्य चिंताएँ*

इन अंतरों के बाद भी चिंतित करने वाले विषय मौजूद हैं। यह भी मुमकिन है कि सरकारों ने इन प्रावधानों को मंजूरी इसीलिये दी क्योंकि यह अध्याय लागू करने लायक नहीं

है। लेकिन भविष्य में यह लागू करने लायक बन सकता है और प्रावधानों की स्वीकृति अन्य वार्ताओं के लिये एक मिसाल के रूप में काम करती है।

RCEP *का स्कोप*

- इस अध्याय का मकसद सिर्फ और सिर्फ ई–कॉमर्स के इस्तेमाल को बढ़ावा देना है। इसमें नियमिक, सामाजिक या मानवाधिकार उद्देश्यों को संतुलित करने की कोई कोशिश नहीं की गई है।

- यह अध्याय उन उन उपायों पर भी लागू होता है जो इलेक्ट्रॉनिक कॉमर्स को प्रभावित करने वाली पार्टी द्वारा अपनाए या स्थापित किये गए हैं। यह सिर्फ उन पर लागू नहीं होता जो सीधे तौर पर इसे निशाना बनाते हैं। अगर हम पहले लीक हुए ड्राफ्ट को देखें, तो पता चलता है कि एक ऐसा ही व्यापक स्कोप सेवाओं के व्यापार के नियमों पर भी लागू होगा, खास तौर पर वित्तीय सेवाओं के नियमों पर। इनकी वजह से डिजिटल और क्रॉस–बॉर्डर सर्विस सप्लायर और गतिविधियों पर अतिरिक्त अवरोध लगने की संभावना पैदा होती है।

- सरकारी खरीद के बहिष्कार का मतलब होता है कि पूरे समझौते की एक सीमित परिभाषा पेश हो रही है। अगर यह आम पैटर्न की तरह जारी रहा, तो यह सिर्फ एक सरकार द्वारा आंतरिक और गैर–व्यवसायी इस्तेमाल के लिए गुड्स और सर्विसेज के खरीद को संदर्भित करेगा।

- 'एक पार्टी की तरफ से रोकी या साझा की गई' जानकारी के बहिष्कार का स्कोप अस्पष्ट है। उदाहरण के तौर पर, यह बात अस्पष्ट है कि यह निजी हित से पैदा किये गए राष्ट्रीय या क्षेत्रीय डेटाबेस को, या एक स्मार्ट सिटी प्रोजेक्ट के तहत एक प्राइवेट फर्म द्वारा इकट्ठा किये गए डेटा को कवर करेगा या नहीं।

- पहले लीक हुई RCEP के निवेश अध्याय से यह पता चलता है कि निवेश अध्याय में कवर किये गए निवेश में निवेश की व्यापक एसेट–आधारित परिभाषा शामिल की जाएगी। मसलन, इंटरप्राइसेज, शेयर, इंटेलेक्चुअल प्रॉपर्टी अधिकार, कॉन्ट्रैक्ट के अधिकार और लाइसेंस।

- वित्तीय सेवा एनेक्स के अनुसार जो वित्तीय संस्थान, सार्वजनिक एंटिटी और वित्तीय सेवा सप्लायर हैं, उन्हें कवरेज से बाहर रखा गया है, साथ ही वित्तीय संस्थान या वित्तीय सेवा सप्लायर के निवेशकों को भी इससे बाहर रखा गया है। हालांकि अभी भी वित्तीय डेटा और विभिन्न तरह के ई–फाइनेंस पर एनेक्स लागू होगा, जो कि उतना ही गलत है।

- TPPA में वित्तीय सेवा नियम उन उपायों पर लागू होते हैं जो वित्तीय सेवाओं की सप्लाई पर असर डालते हैं। इनमें 'वित्तीय जानकारी का प्रावधान और ट्रांसफर, और वित्तीय डेटा की प्रोसेसिंग और अन्य वित्तीय सेवाओं के सप्लायर द्वारा उससे जुड़े सॉफ्टवेयर' शामिल हैं।

- TPPA का एनेक्स 11–B भी है, जो वित्तीय फर्मों के लिए अपने व्यापार के एक सामान्य हिस्से के रूप में स्त्रोत देश से बाहर डेटा ट्रांसफर करने का अधिकार सुनिश्चित करता है।

- सरकारों के पास डेटा प्राइवेसी और गोपनीयता की रक्षा करने के लिए उपाय हो सकते हैं, और उस जानकारी के हासिलकर्ताओं के नियामक स्वीकृति

(विवेकपूर्ण कारणों के लिए) की भी जरूरत हो सकती है– लेकिन एक संभावित सर्कुलर प्रोविजो है कि उन उपायों को इस प्रतिबद्धता या दायित्व से बचने के साधन के रूप में इस्तेमाल नहीं किया जा सकता है! यह स्पष्ट नहीं है कि RCEP में ऐसा कोई प्रावधान है या नहीं। लेकिन अगर ऐसा है, तो वित्तीय विनियमकों (रेगुलेटर्स) के लिए कठिनाइयाँ पैदा हो सकती हैं।

RCEP के अन्य नियम

TPPA के ही कई नियम इसमें जोड़े गए हैं, हालांकि करीब हर नियम बदलाव हुए हैं।

कंप्यूटिंग सुविधाओं का इस्तेमाल और लोकेशन (अनु. 15)

एक कवर किये गए व्यक्ति को एक पार्टी क्षेत्र में वहाँ व्यवसाय करने की स्थिति के रूप में कंप्यूटिंग सुविधाओं जैसे सर्वर का इस्तेमाल करने या खोजने की जरूरत नहीं होनी चाहिये। मुख्य दायित्व TPPA जैसे ही हैं, लेकिन जैसा कि ऊपर बताया गया है, इसमें अपवाद व्यापक हैं।

TPPA की तरह ही, RCEP में एक 'वैध पब्लिक पॉलिसी ऑब्जेक्टिव' हासिल करने के लिए असंगत उपायों को स्वीकृति मिली हुई है। हालांकि यह फैसला RCEP का होगा कि इन उपायों का सेल्फ–जजिंग होना जरूरी है या नहीं। इस बात पर भी बहस हो सकती है कि पब्लिक पॉलिसी ऑब्जेक्टिव वैध है या नही।

TPPA लक्ष्य तक पहुँचने के लिये ऐसे उपाय अपनाता है जिससे उस पर कम से कम बोझ पड़े, वहीं RCEP में क्या उपाय हो, यह पूरी तरह से पार्टियों का फैसला होता है। उपाय को इस तरह से लागू नहीं करना चाहिये कि वह व्यापार पर मनमाने या अनुचित भेदभाव, या अनुचित प्रतिबंध का साधन बन जाये। दोनों ही मामलों में लोकल सर्वर के इस्तेमाल की जरूरत के संदर्भ में यह काफी नुकसानदेह साबित हो सकता है।

हालांकि, इस प्रावधान के विभिन्न पहलुओं को चुनौती दी जा सकती है, मगर यह भी ध्यान रखना जरूरी है कि अभी अध्याय को लागू करने का कोई तंत्र न हो।

इसके साथ ही, कोई भी पार्टी अपने 'जरूरी सुरक्षा हितों' की रक्षा करने के लिए कोई भी जरूरी उपाय अपना सकती है, और इसका स्पष्ट रूप से 'किसी भी पार्टी की तरफ से विरोध नहीं होना चाहिये'।

अंत में, लोकल सर्वर नियम उन उपायों पर लागू नहीं होते जिन्हें सेवा और निवेश क्षेत्र में इस्तेमाल करने अधिकार पार्टी के पास सुरक्षित हैं। यह विभिन्न कारणों से जटिल है। पहला, यह सुरक्षा केवल वहीं तक लागू होती है, जहाँ ई–कॉमर्स नियमों और उन अध्यायों के सुरक्षा पर लागू होने वाले नियमों के बीच क्रॉस–ओवर होता है। (जैसे गैर–भेदभाव) चूंकि हर अध्याय के लिए अलग–अलग वार्ताकार जिम्मेदार हैं, तो यह ऐन मुमकिन है कि उन्होंने अध्यायों के बीच संभावित क्रॉस–ओवर के बारे में नहीं सोचा है। दूसरा, पिछले लीक से पता चलता है कि पार्टियाँ सुरक्षा को ध्यान में रखने के लिए विभिन्न तरह के शेड्यूल का इस्तेमाल कर रही हैं। उन्हें 'नियमों के अधीन क्या है' बताने वाली सकारात्मक सूची से लेकर 'क्या संरक्षित नहीं' बताने वाली नकारात्मक सूची तक संक्रमण करने की जरूरत होती है। यह सूचियाँ तकनीकी लिहाज से बेहद मुश्किल होती हैं, और इनमें गलती या अनदेखे नतीजों का बहुत ज़्यादा खतरा रहता है। उन्हें पार्टियों के बीच समझौते और सहमति की भी जरूरत पड़ती है।

LDC के पास अनुपालन करने के लिए 5 साल हैं, जिसमें 3 साल की बढ़ोतरी हो सकती है। वियतनाम के पास अनुपालन करने के लिए 5 साल हैं।

इलेक्ट्रॉनिक जरिये से जानकारी का क्रॉस–बॉर्डर ट्रांसफर (अनु 16)

इस प्रावधान का आम असर तो TPPA जैसा ही है, लेकिन इसके दायित्व सक्रिय से बदल कर निष्क्रिय हो गए हैं। TPPA ने एक 'कवर किये गए व्यक्ति' को अपने व्यवसाय के लिए जानकारी, जिसमें निजी जानकारी भी शामिल थी, को बॉर्डर पर ट्रांसफर करने की अनुमति देने के लिए एक पॉजिटिव ड्यूटी लगाई थी। RCEP कहता है कि एक पार्टी को ऐसे किसी ट्रांसफर को नहीं रोकना चाहिये।

अनुच्छेद 15, जो लोकल कंप्यूटिंग सुविधाओं पर है, उसके अपवाद इसमें भी मौजूद हैं। सेवाओं और निवेश अध्याय में आरक्षण के लिये भी समान क्रॉस–रेफरेंस लागू होता है।

LDC के पास अनुपालन करने के लिए 5 साल हैं, जिसमें 3 साल की बढ़ोतरी हो सकती है। वियतनाम के पास अनुपालन करने के लिए 5 साल हैं।

इलेक्ट्रॉनिक प्रमाण (अनु 7)

एक कानूनी हस्ताक्षर को सिर्फ इसलिये खारिज नहीं किया जा सकता कि वह इलेक्ट्रॉनिक रूप में है। एक पार्टी के क ायदे–कानून अलग–अलग स्थितियों के लिए अलग नियम हो सकते हैं। कंबोडिया और Lao PDR के पाया अनुपालन करने के लिए 5 साल हैं।

लेनदेन में शामिल निजी पार्टियों को यह निश्चित करने का मौका देना चाहिये कि वह प्रमाणीकरण के लिये कौन सी टेक्नोलॉजी का इस्तेमाल करना चाहती हैं। और यह भी सुनिश्चित होना चाहिये कि यह स्टेट के प्रमाणीकरण संबंधी डोमेस्टिक कानूनों का पालन करें।

सरकारें अपने कायदे–कानून में इलेक्ट्रॉनिक लेनदेन की विशिष्ट कैटेगरी में प्रदर्शन औरध्या प्रमाणीकरण की जरूरत के मानक तय कर सकती हैं। यह कानून RCEP सरकारों को साइबरसिक्योरिटी के कुछ स्तरों को लागू करने से रोकता है। जैसे ऑनलाइन बैंकिंग या क्रेडिट कार्ड डिटेल के एन्क्रिप्शन के लिये टू–फैक्टर प्रमाणीकरण, अगर सरकार ने उन्हें विशेष कैटेगरी में न डाला हो।

कंज्यूमर प्रोटेक्शन (अनु 8)

RCEP की भाषा TPPA प्रावधान से भी ज्यादा कमजोर है। इसमें पार्टियों को कंज्यूमर प्रोटेक्शन उपायों की जरूरत कम से कम ही पड़ती है। इसे बिना कोई न्यूनतम सीमा तय करते हुए, बेहद कमजोर भाषा में यह कह कर परिभाषित किया गया है कि 'यह इलेक्ट्रॉनिक कॉमर्स का इस्तेमाल कर रहे उपभोक्ताओं को धोखाधड़ी या भ्रामक प्रथाओं के खिलाफ सुरक्षित करता है'।

उन्हें यह बात लिखनी चाहिये कि वो किस तरह का कंज्यूमर प्रोटेक्शन देंगे।

टीपीपीए का भी कोई न्यूनतम मानक नहीं है, लेकिन इसे कम से कम ऑनलाइन गतिविधियों में लगे उपभोक्ताओं को नुकसान या संभावित नुकसान पहुंचाने वाली धोखाधड़ी और भ्रामक वाणिज्यिक गतिविधियों के खिलाफ मुकदमा चलाने के लिए उपभोक्ता संरक्षण कानूनों को अपनाने की जरूरत होती है।

LDC के पास अनुपालन करने के लिये 5 साल का समय है।

ऑनलाइन पर्सनल इन्फॉर्मेशन प्रोटेक्शन (अनु 9)

'प्राइवेसी' का प्रावधान भी TPPA के मुकाबले कमजोर है और उससे थोड़ा अलग भी है। पार्टियों के पास एक कानूनी ढांचा होना चाहिये जो 'ई–कॉमर्स के उपभोक्ताओं की निजी जानकारी की सुरक्षा सुनिश्चित कर सके'। निजी जानकारी का मतलब 'किसी भी इंसान के बारे में कोई भी जानकारी या डेटा' होता है।

टीपीपीए को केवल व्यक्तिगत जानकारी के संरक्षण के लिए कानून की आवश्यकता होती है और एक पहचान योग्य नेचुरल व्यक्ति को संदर्भित करता है।

इसका कोई न्यूनतम मानक नहीं है, हालांकि एक पार्टी के लिए यह जरूरी(TPPA में सुझाव दिया गया है) है कि वह जरूरी अंतरराष्ट्रीय संस्थानों के अंतरराष्ट्रीय मानकों, दिशानिर्देशों आदि पर 'नजर बनाये रखे'।

TPPA की बात करें, तो पार्टियाँ एक कंप्रेहेंसिव निजी प्राइवेसी कानून या क्षेत्र–विशिष्ट कानून अपना कर, या एंटरप्राइज द्वारा अपनाए गए अनुबंधीय दायित्वों को लागू करवा के अनुपालन कर सकती हैं।

उनके लिये जरूरी(TPPA ने सुझाव दिया था) है वह संरक्षण के बारे में जानकारी साझा करें और एंटरप्राइज को अपनी पॉलिसी ऑनलाइन छापने के किये प्रेरित करें।

RCEP ने अपने अलग–अलग कानूनी दृष्टिकोणों के बीच अनुकूलता को बढ़ावा देने के लिए 'व्यक्तिगत जानकारी की रक्षा के लिए आर्थिक और सामाजिक लाभ' और पार्टियों के लिए 'प्रोत्साहन' की TPPA की बयानबाजी को खत्म कर दिया है।

LDC के पास अनुपालन करने के लिये 5 साल का ग्रेस पीरियड है।

अनचाहे इलेक्ट्रॉनिक मैसेज (स्पैम) (अनु 10)

पार्टियों को स्पैम पर उपाय अपनाने चाहिये, लेकिन ऐसा मुमकिन है कि यह डिलीवरी के कुछ जरियों जैसे ईमेल तक ही सीमित रह जाएं, और ज्यादा व्यापक फॉर्म जैसे अनचाही एडवरटाइजिंग या टार्गेटेड मैसेजिंग तक न पहुँच पाए।

इन उपायों में जो बिंदु होने चाहिये वह कमजोर हैं : स्पैम भेजने वालों के लिये यह अनिवार्य होना चाहिये कि वह स्पैम पाने वालों को मैसेज रोकने की 'सुविधा' दें, या उनकी मर्जी पूछें, या फिर उन सप्लायर के स्पैम को 'कम करें', जो अनुपालन करने में सक्षम नहीं हैं।

LDC के पास अनुपालन करने के लिये 5 साल का ग्रेस पीरियड है, और ब्रूनेई के पास 3 साल का समय है।

घरेलू नियामक ढांचे (अनु 11)

पार्टियों को इलेक्ट्रॉनिक लेनदेन नियंत्रित करने के लिये एक कानूनी ढांचा तैयार करना चाहिये जो, UNCITRAL, UN या अन्य अंतरराष्ट्रीय कन्वेंशन और ई–कॉमर्स के मॉडल कानूनों पर 'नजर रखने का काम करें'।

कंबोडिया के पास 5 साल का ग्रेस पीरियड है।

पार्टियों को भी 'इलेक्ट्रॉनिक लेनदेन पर किसी भी अनावश्यक नियामक बोझ से बचने के लिए' प्रयास करना चाहिए। हालांकि पार्टी को सिर्फ 'प्रयास' करना चाहिये, बल्कि ऐसा करना उसका सकारात्मक दायित्व भी है। यह सेवाओं के घरेलू विनियमन पर विषयों का एक संस्करण है जिसके लिए विनियमन में हल्के हाथों के दृष्टिकोण की आवश्यकता होती है और जिसका कई विकासशील देशों ने WTO में विरोध किया है।

इलेक्ट्रॉनिक प्रसारण पर कस्टम ड्यूटी (अनु 12)

जैसा कि ऊपर बताया गया है, RCEP कस्टम ड्यूटी पर WTO द्वारा लगाई गई मौजूदा रोक को ही जारी रखता है। हालांकि इलेक्ट्रॉनिक प्रसारण के बारे में कुछ नहीं कहा गया है। इससे यह बात अस्पष्ट रहती है कि क्या यह रोक इलेक्ट्रॉनिक रूप से हस्तांतरण किये गए हर मटेरियल पर लागू होता है (जिसमें कंटेंट भी शामिल है) जैसा कि अमेरिका ने दावा किया है, या फिर यह फिर यह इलेक्ट्रॉनिक रूप से हस्तांतरण किये गए उत्पाद और सेवाओं पर लागू नहीं होता है, जैसा इंडोनेशिया ने WTO सेक्रेटरी जनरल से कहा था। (WT/MIN(17)/68, 20 दिसंबर 2017)

TPPA से अलग, इस रोक को स्थायी नहीं किया गया है। अगर 1998 के ई–कॉमर्स पर WTO वर्क प्रोग्रा (जो एक स्थायी प्रतिबंध हो सकता है, लम्बे समय के लिये हो सकता है, या फिर रोक खत्म होने तक के लिये) का कोई नया निष्कर्ष आया है, तो यह हर RCEP पार्टी पर निर्भर करता है कि वह नई स्थिति को देखते हुए अपना नजरिया बदलेगी या नहीं।

पारदर्शिता (अनु. 13)

पार्टियों को इस अध्याय का अनुपालन करने वाले उपायों को सार्वजनिक रूप से साझा करना चाहिये, कम से कम इंटरनेट पर तो जरूर करना चाहिये। हालांकि यह सिर्फ उतना ही हो 'जितनी जल्दी मुमकिन हो' और 'जहाँ मुमकिन हो'। इसके साथ ही उन्हें दूसरी किसी पार्टी के साथ जल्द से जल्द उन उपायों के बारे में हर वो जानकारी साझा करनी चाहिये।

साइबरसिक्योरिटी (अनु. 14)

TPPA की तरह ही, साइबरसिक्योरिटी के मसले का जिक्र तो है, लेकिन इसे लागू करने का कोई इकरारनामा नहीं है।

अन्य अध्यायों के दायित्व (अनु. 3.5)

ई–कॉमर्स अध्याय यह स्पष्ट कर देता है कि व्यापार सेवाओं और निवेश अध्याय में भी पार्टियों का दायित्व और अन्य संबंधित अपवाद लागू होते हैं। कई कारणों से, वह अध्याय ई–कॉमर्स अध्याय से ज्यादा नुकसानदेह हैं।

सेवाओं में व्यापार का कानून 'सप्लाई पर असर डालने वाले उपायों' पर लागू होता है। ई–कॉमर्स अध्याय में बताए गए कई उपाय यकीनन उस विवरण के अंतर्गत आ सकते हैं, जहाँ किसी पार्टी ने अपने शेड्यूल में (एक सकारात्मक सूची के लिए) प्रासंगिक सेवा की या उसे स्पष्ट रूप से संरक्षित नहीं किया (एक नकारात्मक सूची दृष्टिकोण के तहत)।

कवर की गई सेवाओं में 'कंप्यूटर और कंप्यूटर संबंधी सेवाएँ' शामिल होती हैं। इसमें डेटा प्रोसेसिंग और स्टोरेज, क्षेत्रीय सेवाएं, जैसे कानूनी, वित्तीय, एडवरटाइजिंग, रिटेलिंग और टूरिज्म सेवाएँ शामिल हैं, चाहे वह देश में मुहैया कराई जाएँ, या फिर दूसरे देश में।

यह संभावना है कि सेवा अध्याय एक ऐसा नियम शामिल कर लेगा जिसके तहत सरकारों को देश में लोकल पहुँच बनाने के लिये क्रॉस–बॉर्डर सर्विस सप्लायर की जरूरत नहीं होगी। हालांकि यह उस देश के शेड्यूल आरक्षण पर निर्भर करेगा।

उन सेवाओं के दायित्वों को राज्य–राज्य विवाद निपटान के माध्यम से लागू करना होगा।

गैर–भेदभाव, निष्पक्ष और न्यायसंगत बर्ताव, या प्रत्यक्ष या अप्रत्यक्ष संपत्तिहरण जैसे उपाय जो कथित तौर पर निवेशकों की सुरक्षा का उल्लंघन करते हैं; वह भी राज्य–राज्य और निवेशक–राज्य विवाद निपटान के अधीन हो सकते हैं।