

ПРАВНО РЕГУЛИРАНЕ НА ЕЛЕКТРОННАТА ТЪРГОВИЯ В ПРОГРАМАТА ПО ИНФОРМАЦИОННИ ТЕХНОЛОГИИ ЗА 9. КЛАС ИЛИ... ТОВА, КОЕТО УЧЕБНИКЪТ НЕ КАЗВА

Ангел Стефанов Манчев

СУ „Св. Климент Охридски“, Факултет по журналистика и масови комуникации, София

LEGAL REGULATION OF E-COMMERCE IN THE IT PROGRAM FOR THE 9TH GRADE. WHAT THE TEXTBOOK DOES NOT SAY

Angel Manchev

SU „St. Kliment Ohridski“, Faculty of Journalism and Mass Communication, Sofia

Abstract. Today, as opposed to 10-15 years ago, e-commerce is as something quite ordinary, even weekly. Ecommerce capabilities in terms of access to a huge number of customers even globally, ease of ordering from every point, optimization of business processes, etc. are very attractive. It is logical in a respect that the subject of e-commerce is present in the IT program for the 9th grade for general secondary education. Moreover, although the program includes the requirement for the student to know the basic normative documents relating to e-commerce, this knowledge and understanding of legal regulation seems to be second-tier, leading to significant deficiencies in the aspect of legal thinking formation in future members of the society, not only as regards their online activities but also in their overall behavior. It is right, however, to know that in the online world rules, laws exist with no less power than offline reality, and their knowledge is a key factor for the success of any business venture. That is why in this article we will try to clarify some of the most important issues related to e-business legal regulation such as: Conclusion and validity of online contracts; Providing trader information to users and customers; Protection of consumers' personal data in the context of the new EU rules (GDPR); Intellectual property protection; The legal regulation of e-commerce internationally.

Keywords: legal regulation; e-commerce; IT program for the 9th grade; GDPR; copyright; textbooks

Днес, за разлика от преди 10-15 години, електронната търговия или казано по друг начин – търговията, която се осъществява по интернет, се приема като нещо съвсем обикновено, дори делнично. Сякаш е най-елементарното действие да влезеш през смартфона си в някой интернет магазин, да си избереш стока, да я поръчаш, да я платиш с кредитната си карта и да очакваш доставката ѝ в рамките на ден-два. Определено не звучи трудно, особено в реалност, доминирана от технологиите. И на практика е така! Възможностите на електронната търговия от гледна точка на достъпа до огромен брой клиенти дори в световен мащаб, улеснението при поръчване от всяка точка, оптимизацията на бизнес процесите и т.н., са много привлекателни.

Съвсем логично в аспекта на казаното до тук понятието „електронна търговия“ присъства и в учебната програма по Информационни технологии за 9. клас¹ за общообразователната подготовка в средното училище. Един бърз преглед на програмата показва, че в учебното съдържание електронната търговия следва да присъства като самостоятелна тема в раздел „Компютърни мрежи и услуги“. В рамките на компетентностите, като очаквани резултати от обучението, ученикът трябва да:

- познава основните принципи на електронната търговия;
- посочва областите на приложение на електронната търговия;
- познава основни нормативни документи, свързани с електронната търговия;
- разбира смисъла на понятието електронни пари;
- разбира как се извършват електронни разплащания чрез софтуерни системи в интернет.

Новите понятия, които се въвеждат чрез темата за електронната търговия, съответно, са: електронна търговия и електронно разплащане.

От това следва, че авторите на учебници, трябва да интерпретират и развиват темата според своите виждания и разбирането им за материята.

И макар че, както цитирахме по-горе, в програмата е включено като резултат от обучението изискването ученикът да познава основните нормативни документи, отнасящи се до електронната търговия, това знание и разбиране на правното регулиране сякаш остава на втори план, което води след себе си съществени недостатъци в аспекта на формирането правното мислене у бъдещите членове на обществото ни, не само що се отнася до техните онлайн активности, но и в цялостно им поведение.

Редно е, обаче да се знае, че в онлайн света правилата и законите съществуват и действат с не по-малка сила от офлайн реалността и познаването им е ключов фактор за успеха на всяко бизнес начинание. Ето защо на следващите редове ще се опитаме да изясним някой от най-важните моменти, свързани с правното регулиране при електронния бизнес.

Електронната търговия в България се регулира от нормите на Закона за електронна търговия, Закона за защита на потребителите, Закона за далекосъобщенията, Закона за авторското право, Закона за задълженията и договорите, Наказателния кодекс, Гражданския и гражданско-процесуалния кодекс и др.

Въпреки, че има разлика при електронна търговия между двама търговци (B2B) и между търговец и потребител (B2C), основните аспекти от правна гледна точка, които трябва да бъдат взети предвид, са следните:

Сключване и валидност на договорите онлайн

В електронната търговия неизбежно се налага сключване на договори по интернет, като практиката познава различни видове изразяване на желание и съгласие за сключване на договор – напр. clickwrap, т.е. чрез отбелязване на отметка, например „Съгласен съм с общите условия“, или browwrap – в този случай съгласието се изразява чрез браузване на даден уебсайт. От правна гледна точка, съгласието и моментът на сключване на clickwrap договорите са много по-лесно доказуеми, затова са препоръчителни в сравнение с browwrap.

Трябва да се отбележи, че не всеки вид договор може да бъде сключен онлайн. Договорите, за които се изисква квалифицирана писмена форма за валидност, например нотариална, като договор за продажба на автомобил и договорите, при които физическото притежание на документа има правно значение, например запис на заповед, не могат да бъдат валидно сключени в интернет.

Законът за електронната търговия добавя конкретни изисквания към сключването на договори с електронни средства. Изискват се най-общо три стъпки, като законът прибавя специфики към всяка една от стъпките:

- Предложение за сключване от страна на търговеца (оферта) – на този етап търговецът трябва да укаже ясно техническите стъпки по сключването на договора и тяхното правно значение, дали договорът ще бъде съхраняван от него и какъв е начинът за достъп до него, техническите средства за установяване и поправяне на грешки при въвеждането на информация преди да бъде направено изявлението за сключване на договора, както и езиците, на които договорът може да бъде сключен.
- Изявление за сключване на договор от клиента.
- Потвърждение от страна на търговеца за получаване на изявлението за сключване на договора, например уебстраница, която потвърждава поръчката, имейл и др.

Предоставяне на информация за търговеца на ползвателите и клиентите

В електронната търговия има определен обем информация, която задължително трябва да бъде предоставена на клиента, за да са спазени изискванията на приложимите закони.

От една страна електронната търговия в България се регулира от Закона за електронната търговия (ЗЕТ), който я дефинира като „предоставяне на услуги на информационно общество“. Тук е важно да се отбележи, че законът приема за електронна търговия не всеки вид търговски сделки в интернет, а тези, които са специфични за информационно общество и отговарят на критериите на ЗЕТ (чл. 1, ал. 3). Съгласно ЗЕТ търговецът трябва да предостави следната информация на достъпно място на уебсайта си:

- името или наименованието си;
- постоянния си адрес или седалището и адреса си на управление;
- адреса, на който упражнява дейността си, ако е различен горния;
- данни за кореспонденция, включително телефон и имейл;
- данни за вписване в търговски или друг публичен регистър;
- съответно указание, ако е регистриран по Закона за данък върху добавената стойност (ЗДДС);
- когато се посочват цени, те трябва да се обозначават по ясен и разбираем начин.

Защита на личните данни на потребителите

Към днешна дата защитата на личните данни представлява една от най-актуалните и дискутираните теми в обществото. От 25 май 2018 г. са в сила новите правила за лични данни на Европейския съюз, които националните органи на всяка държава членка, включително и България, трябва да внедрят във вътрешното си законодателство. Те са уредени в т.нар. Общ регламент за защита на личните данни (GDPR)². Новата правна рамка запазва редица основополагащи принципи и понятия от съществуващата към момента нормативна уредба, но в същото време въвежда по-високи стандарти за защита на данните, разширени права на физическите лица и нови задължения на администраторите на лични данни. Държавите трябва да осигурят на националните си органи необходимите финансови и човешки ресурси, за да се гарантират тяхната независимост и ефикасност. Целта на тези правила е да бъде защитена неприкосновеността на личния живот на европейците и да се засилят доверието и сигурността на потребителите, като същевременно се открият нови възможности за предприятията, особено за по-малките. Това на практика означава, че всеки един бизнес трябва да се подготви за тях, защото в противен случай рискува огромни глоби.

В насоките Европейската комисия са дадени основните елементи на новите правила за защита на данните, а именно:

- Единен набор от правила за целия континент, гарантиращ правна сигурност за предприятията и еднаква степен на защита на данните за гражданите в целия ЕС.
- Еднакви правила, приложими по отношение на всички дружества, които предлагат услуги в ЕС, дори ако седалището на тези дружества се намира извън ЕС.
- По-големи и нови права за гражданите: правото на информация, правото на достъп и правото „да бъдеш забравен“ са засилени. Ново право на преносимост на данните позволява на гражданите да прехвърлят своите данни от едно дружество в друго, което ще открие нови възможности за стопанска дейност на предприятията.
- По-силна защита срещу нарушенията на сигурността на личните данни: дружество, по отношение на което е нарушена сигурността на данните и което излага на риск дадени лица, трябва да уведоми за това органа за защита на данните в срок от 72 часа.
- Строги правила и възпиращи глоби: всички органи за защита на данните ще разполагат с правомощието да налагат глоби до 20 милиона евро, или когато става дума за предприятия - в размер на 4 % от годишния оборот на компанията.

Основните моменти според Общия регламент за защита на личните данни са³:

- Съгласие за обработване на лични данни. Съгласието е едно от алтернативните основания за законосъобразно обработване на лични данни. В случай, че администраторът реши да обработва данните на това основание, той следва да е в състояние да докаже, че съгласието е: свободно изразено; конкретно; относимо; информирано; недвусмислено; дадено с активно действие, вкл. онлайн.
- Правото да бъдеш забравен. Правото на изтриване или „правото да бъдеш забравен“ дава възможност, когато субектът на данни не желае данните му да бъдат обработвани и не съществуват законни основания за тяхното съхранение, да поиска те да бъдат заличени при определени основания. „Правото да бъдеш забравен“ не е абсолютно право. Съществуват ситуации, в които администраторът има възможност да откаже да изтрие данните, а именно когато обработването на конкретните данни е необходимо за някоя от специално изброените в Общия регламент цели.
- Профилиране. Профилиране е автоматизирано обработване на лични данни в онлайн среда, с цел оценяване на определени лични аспекти, свързани с дадено лице, вкл. за анализиране или прогнозиране на поведението му, изпълнението на професионалните му задължения, икономическото му състояние, здраве, лични предпочитания, интереси, надеждност, поведение, местоположение или движение.
- Длъжностно лице по защита на данните. Длъжностното лице по защита на данните играе ключова роля за осигуряване на законосъобразното обработване на лични данни в структурата на администратора. То трябва да разполага с професионални качества и експертни познания в областта на защитата на личните данни - законодателство и практика. Основната задача на длъжностното лице е да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни. Важно е да се знае, че то не определя целите и средствата за обработване на данни и съответно администраторът не може да прехвърли своята отговорност за неспазване на изискванията на Общия регламент върху него.

- **Отчетност.** Отчетността е ново задължение на администраторите на лични данни и основен инструмент за доказване изпълнението на изискванията на Общия регламент за защита на личните данни. Отчетност на практика е способността във всеки един момент администраторът на лични данни да удостовери и да докаже, че обработва личните данни законосъобразно, добросъвестно, прозрачно, за конкретни и пропорционални цели, с подходящо ниво на сигурност и защита.
- **Оценка на въздействието.** Оценката на въздействието е важен инструмент за отчетност, тъй като помага на администраторите не само да спазват изискванията на Общия регламент за защита на личните данни, но и да демонстрират, че са взети подходящи мерки, за да се гарантира спазването на регламента.
- **Защитата на личните данни на етапа на проектирането (privacy by design) и по подразбиране (privacy by default).** Защита на личните данни на етапа на проектирането се изразява в задължението на администраторите да въведат подходящи технически и организационни мерки преди започването на обработката на лични данни, на етапа определяне на целите и средствата за обработване, като осигурят тяхното прилагане през целия жизнен цикъл на данните. Това задължение е от съществено значение в контекста на новите технологии и предоставянето на услуги на информационното общество.
- **Административно-наказателна отговорност по Общия регламент за защита на личните данни.** Един от основните механизми за гарантиране спазването на високите стандарти на регламента от всички администратори, които са задължени да прилагат Регламент 2016/679, е възможността надзорните органи по защита на личните данни да налагат значителни по размер административни наказания – до 20 млн. евро или до 4% от общия годишен световен оборот, която от двете суми е по-висока.

Лични данни са всяка информация, отнасяща се до физическо лице, което е идентифицирано или може да бъде идентифицирано пряко или непряко чрез идентификационен номер или чрез един или повече специфични признаци. Например това са: имена, ЕГН, адрес, телефон, месторождение, паспортни данни на лицето (физическа идентичност); семейно положение и родствени връзки (семейна идентичност); професионална биография (трудова дейност); здравен статус, психологическо и/или умствено състояние, сексуална ориентация (медицински данни); расов или етнически произход, политически, религиозни или философски убеждения (обществена идентичност); имотно състояние, финансово състояние, участие и/или притежаване на дялове или ценни книжа на дружества (икономическа идентичност) и др.

Всеки, който може да бъде класифициран като администратор на лични данни съгласно Закона за защита на личните данни (чл. 3 ал. 1 и 2) трябва да се регистрира като такъв в Комисията за защита на лични данни. При извършване на електронна търговия, в почти всички случаи търговецът попада в дефиницията за администратор, затова подаването на заявление за регистрация е важно изискване, което не трябва да се пропуска. Заявление за регистрация се подава в КЗЛД преди започване обработването на лични данни, а не след това.

Във връзка с личните данни много удобно е използването на Политика за поверителност (**Privacy Policy**), която да се постави на видно място на уебсайта – документ, който често случу като допълнение към Общите условия в частта защита на личните данни и представя как конкретният търговец обработва личните данни на клиентите си. Както и с Общите условия, е добре да е изготвена специално за конкретният случай, защото рискът да е неприложима към ситуацията е голям.

Защита на интелектуалната собственост

А. Защита на своето авторско право

Правото на автора по отношение на обектите, които е създал, възниква автоматично в момента на създаване на обекта, например статия, снимка, дизайн на уебсайт, сорс код на софтуер и др., и обективизираното му на материален носител, т.е. написване на хартия, публикуване в интернет и т.н. и дори нематериализираните произведения като речи, проповеди, изявления и др., без да е необходимо обектът да се регистрира някъде.

Въпреки това с цел доказване на авторството, както и началния момент на авторството, е добре да са налични документи с точна дата, които установяват кой е носителят на правата.

Според българското законодателство е задължително да има сключен писмен договор с разработчика на уебсайт, в който да се уговори, че необходимите права за използване се притежават от поръчителя, а самото предаване да се документира с приемо-предавателен протокол. Същото важи и за авторите на всички останали обекти на интелектуална собственост, например снимки, лого и т.н.

Разбира се най-удобният вариант от гледна точка на защита правата на интелектуална собственост е или търговецът сам да разработи уебсайта си, както и други обекти на интелектуална собственост или, когато това не е възможно, те да бъдат изработени от негови служители, с които се намира в трудово правоотношение, тъй като тогава авторското право възниква директно за работодателя, когато се разработва софтуер.

Б. Спазване на чуждото авторско право

Освен, ако изрично не е указано, че даден обект е освободен от права на интелектуална собственост от страна на автора, трябва да се приеме, че всяко произведение като статия, снимка, дизайн на уебсайт, код на софтуер, песен и др., създадено от друго лице, е защитено като обект на авторско право. Това означава, че за търговски цели, може да бъде използвано само с изричното разрешение на автора или носителя на правата. Напр. снимка, която е свободно достъпна в интернет, в общия случай не е лишена от авторски права, и за използването ѝ е необходимо разрешението на автора.

Правното регулиране на електронната търговия в международен план

Какво се случва при спор, ако търговецът е юридическо лице, регистрирано в България, сървърите му са в Индия, а клиентите му са предимно потребители от САЩ? Законите на коя държава ще се прилагат (приложимо право) и кой съд ще отсъди по този спор (подсъдност)?

Всеки подобен случай изисква конкретно разглеждане и консултация със специалист, но най-общо е важно да се знае, че страните имат относителна автономност сами да изберат:

А. Приложимо право

Business to Business (B2B)

Когато и двете страни са търговци от различни държави, те могат свободно да изберат правото на коя държава ще се прилага спрямо техните отношения. Когато не са избрали, с някои изключения се прилага държавата по мястото на дейност на доставчика, т.е. принципът Country of Origin. Мястото на дейност не е местонахождението на оборудването, нито държава, в която уебсайтът е достъпен, а обикновено е там, където е регистрирано юридическото лице. При електронната търговия, най-удобно е търговецът да включи клауза за избор на право в уебсайта си, например в общите условия.

Business to Consumer (B2C)

Когато обаче една от страните е потребител, т.е. физическо лице, има специфични правила. Отново страните имат право на избор, но в общия случай изборът не трябва да лишава потребителя от защитата, дадена му от императивните правила на правото на държавата на неговото гражданство или обичайно пребиваване.

Б. Подсъдност

Business to Business (B2B)

Тук отново страните са свободни да избират, а когато не са се възползвали от възможността за избор, компетентен е съдът по местожителството на ответника или мястото на изпълнение на договора. Затова, както и с приложимото право, е препоръчително да се включи клауза за избор на подсъдно право на видно място в уебсайта, например в общите условия.

Business to Consumer (B2C)

Съществува допълнителна защита за потребителя. Страните са свободни да изберат подсъдността, но при спазване на определени условия. При липса на договорна клауза, подсъдността зависи от това кой иницира съдебния спор: потребителят може да избира между своята държава или държавата според място на дейност на доставчика, а доставчикът – единствено в държавата на потребителя.

От казаното до тук може да се заключи, че има пряка връзка между стремглавото развитие на електронната търговия и наличието и спазването на определени правила, зададени под формата на нормативни документи, които формират правното регулиране в този сектор.

Изключителните бизнес възможности на интернет за развиване на принципно нови и усъвършенстването на познатите до сега схеми за взаимодействие между отделните звена на пазара, допълват традиционните канали на дистрибуция и се характеризират с ниски разходи, непрекъснати операции и връзка с клиентите при висока прецизност. Към потребителската база от данни се добавят нови клиенти, които не биха могли да бъдат достигнати по традиционните начини. Много често това е свързано и с пълно вътрешно реструктуриране на работата в самото предприятие, като опериране 24 часа на ден, 7 дни в седмицата, 365 дни в годината.

Но и на теоретиците и на практиците в тази област е добре известно, че за да се развива електронната търговия трябва да са на лице най-малко четири важни условия:

- гъвкава правна рамка на електронните комуникации;
- сигурна комуникационна среда;
- условия за осъществяване на сделки и разплащания онлайн;
- умения за ползване на новите възможности за комуникация и обмен.

Адекватното правно регулиране на електронната търговия, обаче е от първостепенно значение, защото то е единственият начин да се опази и доверието на клиентите, а именно доверието е един от най-значимите фактори за осъществяването на всяка търговската дейност.

(Endnotes)

1. Учебна програма по информационни технологии за 9. клас [онлайн]. [прегледан 15.07.2018]. file:///C:/Users/user-pc/Downloads/UP_IT_9kl%20(2).pdf
2. GDPR Portal: Site Overview [онлайн]. [прегледан 15.07.2018]. <https://www.eugdpr.org/>
3. Разяснения относно практическото приложение на Общия регламент за защита на данните от органите на местното самоуправление [онлайн]. [прегледан 15.07.2018]. <https://www.cdpd.bg/?p=element&aid=1127>